

Module 1 – Understanding Computer Hardware



*U.S. Department of
Homeland Security*

United States
Secret Service

You will learn ...

- Safety Overview
- Overview of Computers
- Motherboards and Components
- CPU and Memory



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 1 – Safety Briefing

- Safety Briefing
- Step-by-step Safety Procedures



*U.S. Department of
Homeland Security*

United States
Secret Service

Safety Briefing

- The need for safety procedures
- Work involves disassembly and reassembly of computer components
- All electrical devices contain components that may injure or kill



*U.S. Department of
Homeland Security*

United States
Secret Service

Step-by-Step Safety Procedures

Step 1: Turn off power and disconnect main power cables

Step 2: Use a wrist grounding strap and electrostatic mat

Step 3: Remove all jewelry from hands



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 2 - Overview of Computers

- Introduction
- History of Computers
- Basic System Components



*U.S. Department of
Homeland Security*

United States
Secret Service

Overview of Components

- Computer is a machine that performs high-speed operations and processes data
- Collection of electronic switches, or transistors, operating very quickly in a specific order
- Programs tell transistors how, when, and in what order to turn on and off
- On and off actions equate to binary system of numbers 1 (On) and 0 (Off)



*U.S. Department of
Homeland Security*

United States
Secret Service

Overview of Components

- Computer programs consist of streams of bits indicating on and off
- Streams referred to as data stream or a bit stream
- Computers only recognize information in bits called machine language
- Software and hardware translate numerical streams into a human readable format



*U.S. Department of
Homeland Security*

United States
Secret Service

Overview of Components

- Computers range in function from general purpose desktop PC to massive mainframes to specialized chips in children's toys
- Most prevalent is PC
- Consists of a case that sits on floor or desk, a monitor, a keyboard, and various peripherals like printers
- Functions range from general purpose, stand-alone systems to specialized servers that perform networking operations



*U.S. Department of
Homeland Security*

United States
Secret Service

Laptops and Notebooks

- Laptop and notebook computers are designed to be portable
- Early models heavy, slow, and lacking storage capacity of desktop counterparts
- Many rival performance of most desktop PCs



*U.S. Department of
Homeland Security*

United States
Secret Service

Laptops

- Typically weigh seven pounds or less and are approximately 9x12x2 inches in size
- Powered by rechargeable batteries and AC adapters
- Can offer high performance and multimedia capabilities
- Docking station can be added to enable connectivity to networks, regular monitors, keyboards, and other peripherals



*U.S. Department of
Homeland Security*

United States
Secret Service

Notebooks

- Smaller and lighter than a laptop
- Lack high-end multimedia functions of laptops
- Many have comparable hard drive and memory configurations and are equipped with sound and CD-ROM drives



*U.S. Department of
Homeland Security*

United States
Secret Service

Personal Digital Assistants (PDAs)

- Known as palm pilots, IPAQs, and pocket PCs, they meet demand for reduced-function portable computer
- Enable users to manage files and swap data with a Windows PC
- Used to maintain contact lists and track appointments
- Manage e-mail, paging, and faxes
- Wireless connectivity to other devices using infrared connection



*U.S. Department of
Homeland Security*

United States
Secret Service

Personal Digital Assistants (PDAs)

- Connect to Internet through wireless modems
- Removable flash memory cards
- Double as cell phone
- Most intended to synchronize with home or office workstations
- Usually cannot permanently store data
- Lose any data stored in memory if battery power lost
- Battery charger essential to safeguarding stored data



*U.S. Department of
Homeland Security*

United States
Secret Service

Telephones

- Three phone types include cell, cordless, and direct connect to a landline system
- Provide communication using landlines, radio transmission, cellular systems, or a combination
- Many phones programmable and capable of storing names and phone numbers
- Cellular phones can store appointments, e-mail, pages, voice mail, and passwords



*U.S. Department of
Homeland Security*

United States
Secret Service

Phone Answering Machine

- Can be integral part of phone or separate unit that connects phone to a landline
- Records voice messages from callers using either magnetic tape or digital system
- Can store phone numbers and names, voice recordings, deleted messages, time/date information, memos, and caller IDs



*U.S. Department of
Homeland Security*

United States
Secret Service

Fax Machines

- Transmit and receive documents over phone system
- Memory capacity to store scanned outgoing documents prior to transmission and incoming pages prior to printing
- Can store pre-programmed phone numbers, document pages, and a send/receive log



*U.S. Department of
Homeland Security*

United States
Secret Service

Digital Cameras

- Capture images that frequently have associated date and time stamps
- May have built-in memory, which may be expanded using flash ROM cards
- Can store images in dozens of formats, including any kind of file(s) stored from a computer



*U.S. Department of
Homeland Security*

United States
Secret Service

History

- Blaise Pascal's Arithmetic Machine automated subtraction and addition computations
- Charles Babbage invented concept of Analytical Engine
- Could make decisions for sequential control, branching, and looping based on its own computations
- Early machines used gears
- Electricity added as a signaling medium, machines used switches and electro-mechanical relays for computations



*U.S. Department of
Homeland Security*

United States
Secret Service

History

- Mid 1940s, first electronic computers used vacuum tubes instead of switches
- Vacuum tubes could turn on and off much faster than earlier machines
- Very inefficient, slow, required large amounts of electricity and space, and generated large amounts of heat
- ENIAC (Electronic Numerical Integrator Analyzer and Computer)



*U.S. Department of
Homeland Security*

United States
Secret Service

First Transistors

- Small, solid-state electronic switch, first invented in 1929 and manufactured in 1947 by Bell Labs
- First semiconductor transistor, no moving parts, one-fifth size of the vacuum tube, one hundred times faster
- Early 1950s, Texas Instruments producing silicon transistors, paved way for small modern computer
- IBM started selling Model 650 computer to a few government agencies and commercial businesses



*U.S. Department of
Homeland Security*

United States
Secret Service

The Integrated Circuit (IC)

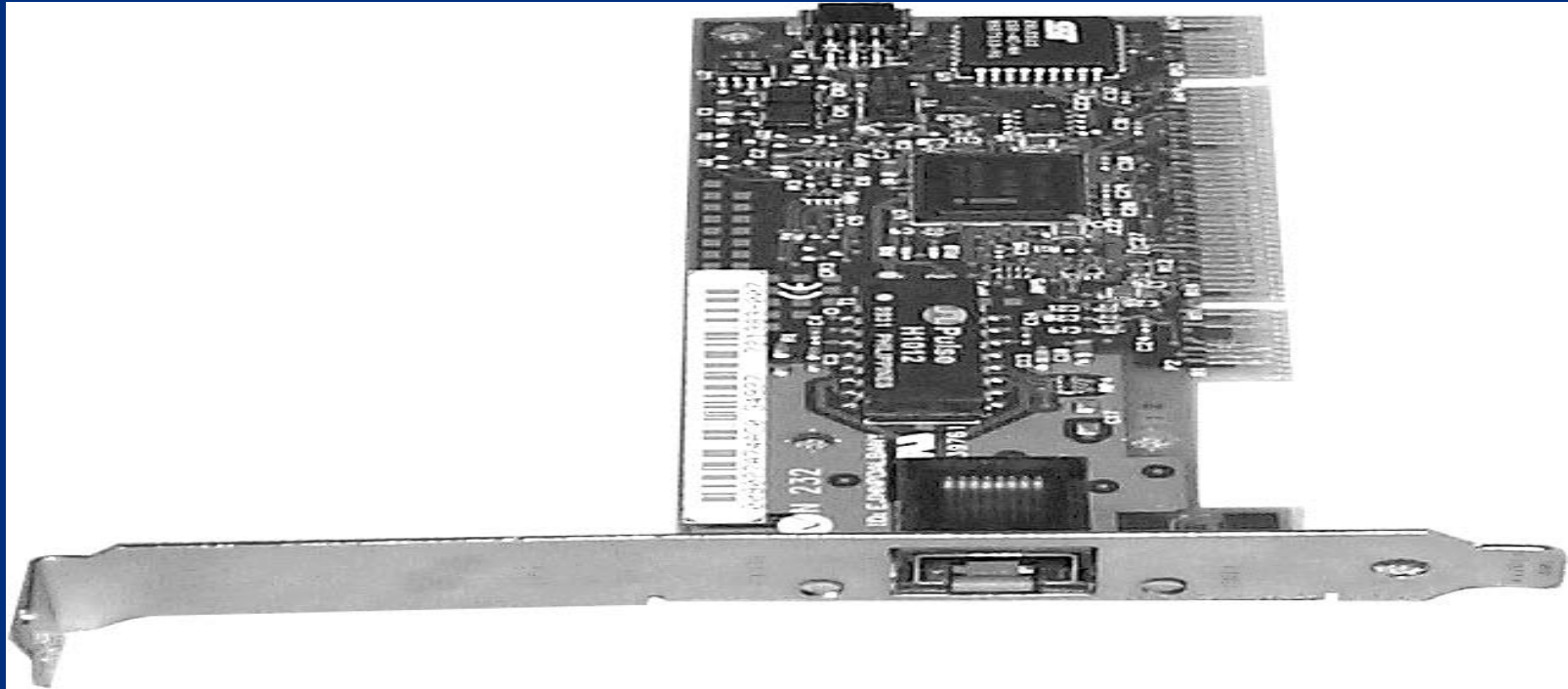
- Invented by Texas Instruments in 1959, integrated circuit (IC), enhanced computer performance
- First IC contained several transistors and circuitry connected by layers of semiconductor (silicon) material
- Connection paths etched into the silicon “chip” with acid or lasers
- Refinements led to miniaturized integrated circuits, many more tiny transistors placed on single silicon chip
- Microprocessor, developed during the 1970s, can contain several million transistors



*U.S. Department of
Homeland Security*

United States
Secret Service

Printed Circuit Board with Integrated Circuits



*U.S. Department of
Homeland Security*

United States
Secret Service

The Growth of Personal Computers

- With Integrated Circuit technology came smaller and cheaper computers
- First personal computer (PC) debuted in 1975, Altair 8800
- Sold as kit, contained an Intel 8080 microprocessor and 256 bytes of RAM
- Built without keyboard or monitor
- Users flipped switches on front panel to input data and programs



*U.S. Department of
Homeland Security*

United States
Secret Service

The Growth of Personal Computers

- Altair displayed output on rows of small lights called light-emitting diodes (LEDs)
- Demand grew, manufacturers make computers user-friendly by adding keyboards, video displays, and data storage devices
- 1976, Apple computer first PC considered powerful enough to be used by businesses and average consumers



*U.S. Department of
Homeland Security*

United States
Secret Service

The Growth of Personal Computers

- IBM, Radio Shack, and Commodore offer new products for both business and home use
- CPUs more powerful and offered increased computational abilities
- Graphical user interfaces (GUI) made new microcomputers user-friendly



*U.S. Department of
Homeland Security*

United States
Secret Service

Basic System Components

- Main system components
- Data storage and retrieval components
- Input components
- Output components



*U.S. Department of
Homeland Security*

United States
Secret Service

Main System Components

- Motherboard (MB)
 - Printed circuit board holds memory chips, expansion cards, and various other components
- Central Processing Unit (CPU) (Brains of computer)
 - Uses microchip technology to process information and code used by computer
- Bus (computer's nervous system)
 - Common pathway, data and power signals travel over to various computer components



*U.S. Department of
Homeland Security*

United States
Secret Service

Main System Components

- Chipset
 - Main circuit of the MB, controls many different components of system
- Memory
 - Stores everything system is processing at a given time
 - Random access memory (RAM), short-term memory
 - Read-only memory (ROM), hard-coded memory that is ever-present



*U.S. Department of
Homeland Security*

United States
Secret Service

Main System Components

- Power Supply
 - Provides power to every piece of hardware in computer case, converts voltage from wall outlet to level computer can use safely
- Cooling Fans
 - Fans force air into case and over components to cool them
- Chassis
 - Computer's case that houses system's internal components



*U.S. Department of
Homeland Security*

United States
Secret Service

Data Storage/Retrieval Components

- Hard Drive
 - Main data repository for non-volatile mass storage
 - Uses magnetically coated metal, glass or ceramic platters as storage media
- Floppy Drive
 - Portable semi-mass storage
 - Uses 3.5 inch floppy disks



*U.S. Department of
Homeland Security*

United States
Secret Service

Data Storage/Retrieval Components

- CD-ROM/DVD
 - Non-volatile, optical mass storage device
- PC Card
 - Versatile, solid-state storage device, can be used as additional hard drive, RAM, or communications device used in laptops, notebooks, and select PDAs



*U.S. Department of
Homeland Security*

United States
Secret Service

Input Components

- Keyboard
 - Primary input device, uses alphanumeric keys
- Mouse
 - Device that moves pointer to make selections in a GUI
- Game Controller
 - Joystick or other device used to play games
 - Require a game controller card or sound card, chip, or chipset with game controller port



*U.S. Department of
Homeland Security*

United States
Secret Service

Output Components

- Monitor
 - Main display component that interactively shows visual input/output
 - Requires video card or video chip/chipset
- Video Card, Chip, Chipset
 - Translates visual input/output and sends to monitor
 - Components are found on MB



*U.S. Department of
Homeland Security*

United States
Secret Service

Output Components

- Speakers
 - Carry audio data processed by sound card or chipset
 - May be attached to sound card by cables mounted in chassis and connected directly to MB, PC speaker, or both
- Sound Card and Chipset
 - Translates audio input/output (I/O) and sends it to speakers
 - Both found on MB



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 3 – Motherboard and Components

- Motherboard Overview
- Motherboard Components
- The Boot Process
- Bus Overview
- Bus Types



*U.S. Department of
Homeland Security*

United States
Secret Service

Motherboard Overview

- Main circuit board of computer
- Every component connected in some way
- Contain slots that hold processor, expansion cards, and connectors for attaching additional boards
- CPU
- ROM (System BIOS)
- Serial and parallel ports
- Memory



*U.S. Department of
Homeland Security*

United States
Secret Service

Motherboard Overview

- Chipset
- Clock and Complementary Metal Oxide Semiconductor (CMOS) battery
- Mass storage interface
- Expansion slots
- Connectors for peripherals including monitor, keyboard, and disk drive(s)
- Vista Specific (Screen-duo and ReadyBoost)



*U.S. Department of
Homeland Security*

United States
Secret Service

Types of Motherboards

- Several different *form factors* (designs) of MBs
- Older form factors include Baby-AT, first IBM PC board released in 1981, Full-size AT, and LPX
- Modern form factors found in most computers today include the NLX, BTX and ATX family of form factors, namely the Micro-ATX, Flex-ATX, and WTX



U.S. Department of
Homeland Security

United States
Secret Service

Types of Motherboards

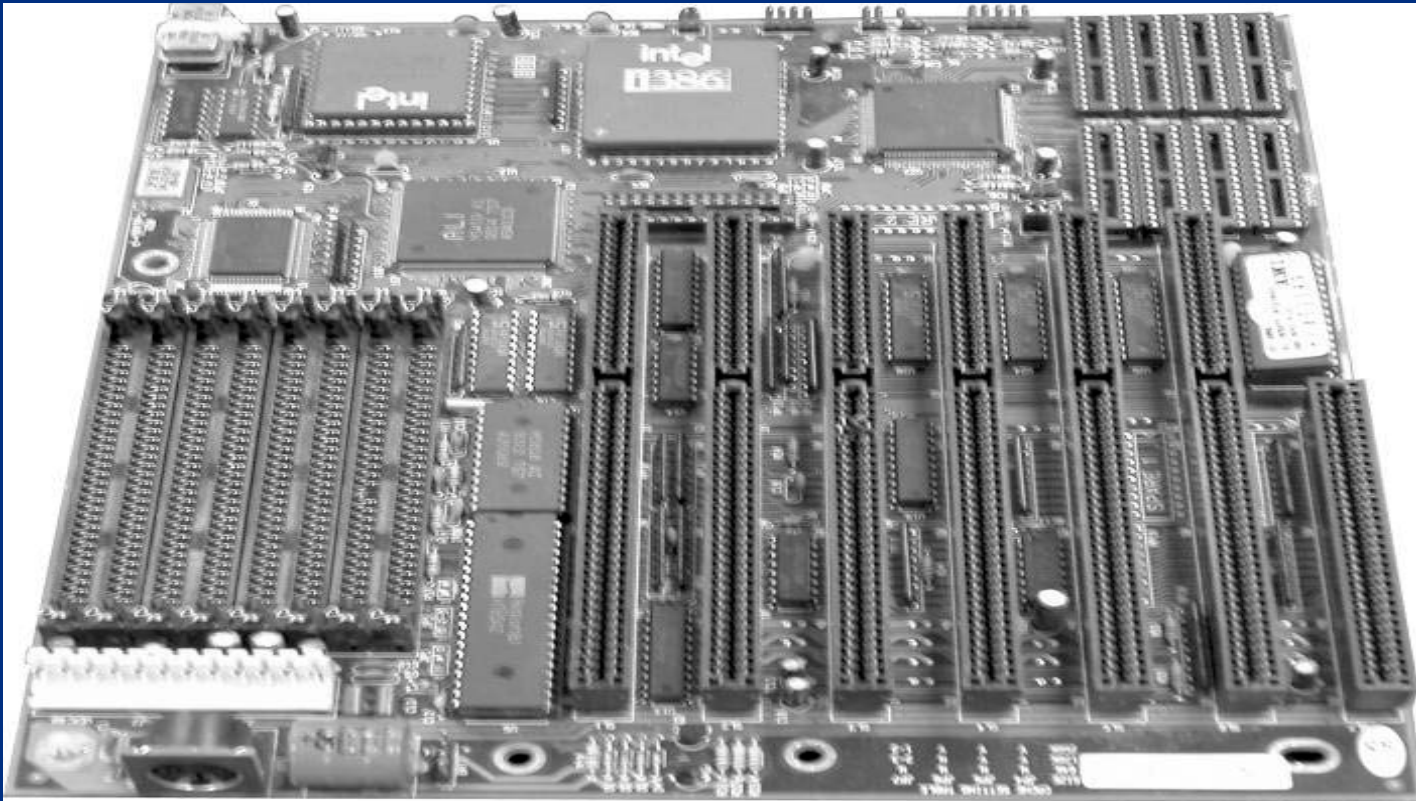
- Full-size AT MB replaced original IBM XT MB in 1984
- Initially large board measuring 12 inches wide by 13.5 inches long, reduced in size as advancements in design progressed
- Contains two power supply connectors that plug into one non-form molded power connector and combination of 16-bit and/or 8-bit ISA slots



*U.S. Department of
Homeland Security*

United States
Secret Service

Example of AT Motherboard



*U.S. Department of
Homeland Security*

United States
Secret Service

Types of Motherboards

- In 1996 Intel introduced ATX as replacement for Baby-AT
- Considered first dramatic improvement in MB form factors used in desktop PCs
- ATX provided standard, nonproprietary design, easy to install and maintain
- Modern MBs use same form factor (9 inches wide by 12 inches long)
- First to integrate components such as Flash BIOS and I/O logic



*U.S. Department of
Homeland Security*

United States
Secret Service

Types of Motherboards

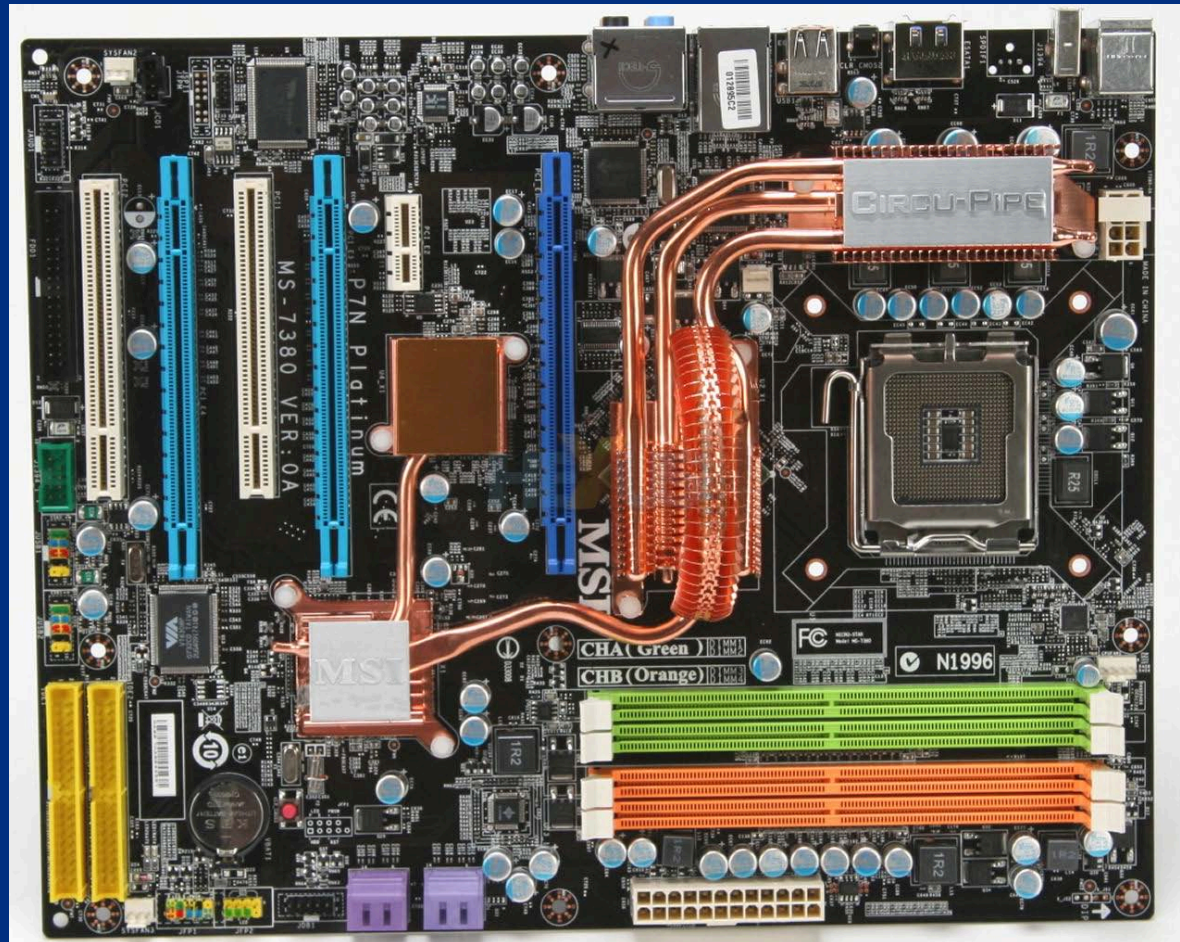
- ATX MB half the width of earlier MBs and contains combination of ISA and PCI slots
- Power connector for ATX is one form-molded power connector that prevents it from being connected incorrectly
- ATX-class and above MBs may be configured for suspend or power-off functions initiated by operating system



*U.S. Department of
Homeland Security*

United States
Secret Service

Example of ATX Motherboard



U.S. Department of
Homeland Security

United States
Secret Service

The ATX Family

- ATX form factors developed by Intel as evolutions of original ATX:
 - Flex ATX
 - Micro ATX
 - WTX



*U.S. Department of
Homeland Security*

United States
Secret Service

Low Profile Extended (LPX) Board

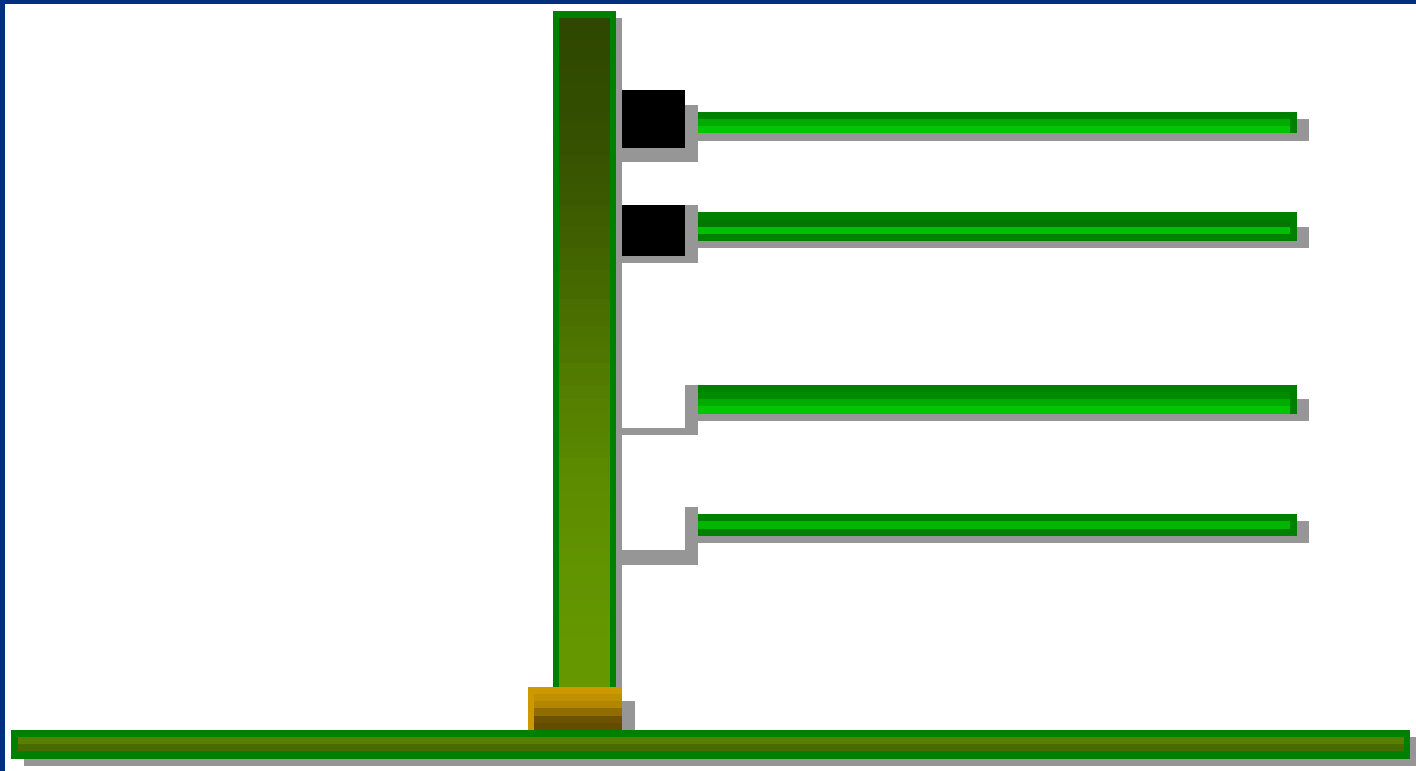
- LPX is semi-proprietary, non-standard design introduced by Western Digital in 1987
- Incorporates slots parallel to MB allowing expansion cards to plug sideways into riser board
- Riser board connects to MB
- Design change allowed for slimmer PC cases
- Used in PCs sold in retail stores such as Compaq and Packard-Bell
- Easy to identify, devices parallel to MB



*U.S. Department of
Homeland Security*

United States
Secret Service

Riser Board Example



*U.S. Department of
Homeland Security*

United States
Secret Service

New Low Profile Extended (NLX) Board

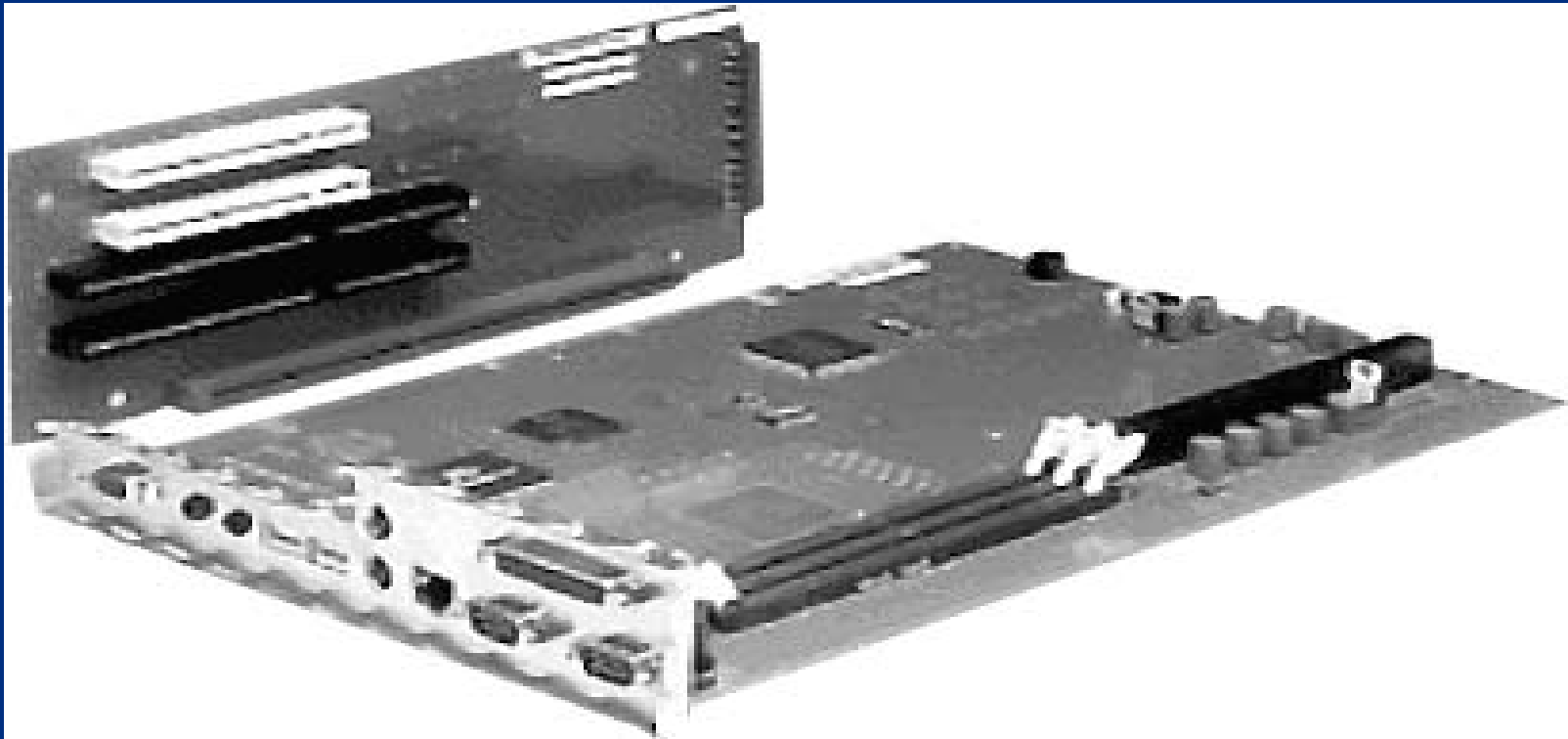
- NLX is a modified, non-proprietary LPX design made by Intel
- With NLX system, riser plugs into side of MB
- Configuration allows easy access to components for installation and maintenance
- NLX has integrated network interface card (NIC)



*U.S. Department of
Homeland Security*

United States
Secret Service

Example of NLX Motherboard with Riser



*U.S. Department of
Homeland Security*

United States
Secret Service

Motherboard BIOS

- Considered heart of computer, controls communications between computer hardware and operating system
- System BIOS, also referred to as ROM BIOS because code is contained in a non-volatile, ROM chip
- Contains software instruction set called firmware
- *Firmware* provides basic input/output instructions to boot computer and handles several important functions



U.S. Department of
Homeland Security

United States
Secret Service

Complimentary Metal Oxide on Semiconductor (CMOS)

- Chip that stores clock settings, current system configuration data as discovered by POST or defined by setup program, and Plug and Play settings
- Located on MB
- Volatile, requires battery power to maintain CMOS memory and system time whether PC is on or off



*U.S. Department of
Homeland Security*

United States
Secret Service

Complimentary Metal Oxide on Semiconductor (CMOS)

- Battery power comes from one of following:
 - Coin-type watch battery (commonly used)
 - Brick/Barrel type battery
 - Capacitor, an electrical component that holds a charge
- Data stored in CMOS chip accessed by system BIOS, includes configurable settings such as boot sequence, CPU clock speed, and power management



*U.S. Department of
Homeland Security*

United States
Secret Service

Chipset

- Controls flow of information between various components of MB
- Chipset on modern PC contains two or three separate chips, older PCs had as many as five chips
- Largest chip is called North Bridge; smaller chip is called South Bridge



*U.S. Department of
Homeland Security*

United States
Secret Service

Chipset

- Controls many different components of system including:
 - CPU
 - Cache
 - Main memory
 - Peripheral Component Interconnect (PCI) bus
 - Industry Standard Architecture (ISA) bus
 - Various system resources



*U.S. Department of
Homeland Security*

United States
Secret Service

Chipset

- Defines various functions the system will support including:
 - Defines Front-side Bus speed (66, 100, 133, or 266-plus MHz)
 - Supports Accelerated Graphics Port (AGP) video cards
 - Defines minimum and maximum processor speed MB can handle
- Major chipset manufacturers, Intel, Apollo, VIA, and SIS



*U.S. Department of
Homeland Security*

United States
Secret Service

Super I/O Chip

- Chip on MB that integrates devices that were contained on expansion cards on older PCs
- Allows for faster transfer rate of data between device and system and has lower failure rate
- Usually contains the following devices:
 - Dual serial port controllers
 - Floppy drive controller
 - Parallel port controller
 - Keyboard and mouse controllers



*U.S. Department of
Homeland Security*

United States
Secret Service

Jumpers

- Small plastic-covered metal clip placed over metal pins sticking out of board
- Enables electricity to flow to pins, completing circuit
- Considered closed when plastic clip covers pins
- Used to control device settings including processor speed and type, bus speed and CMOS password settings

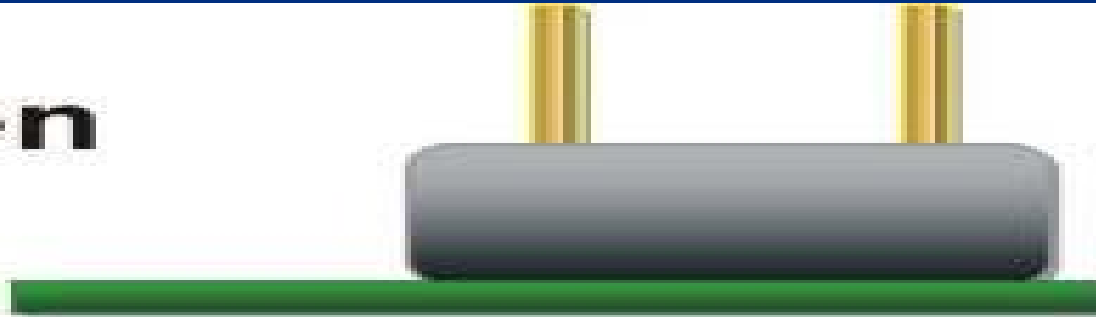


*U.S. Department of
Homeland Security*

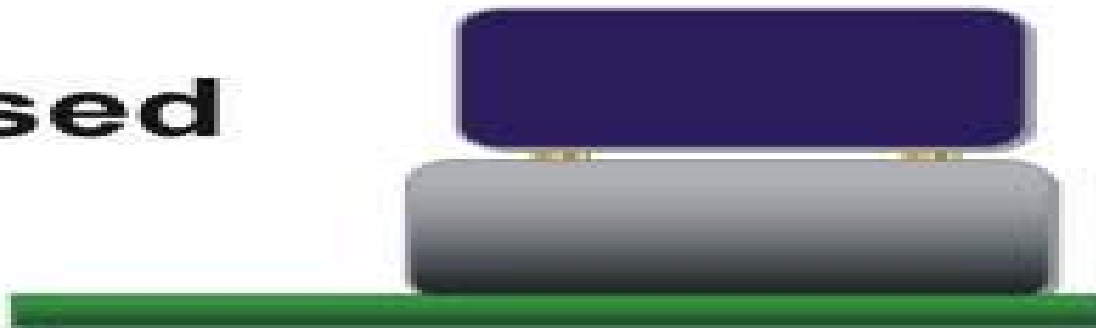
United States
Secret Service

Jumpers

Open



Closed



*U.S. Department of
Homeland Security*

United States
Secret Service

Dual Inline Package Switches

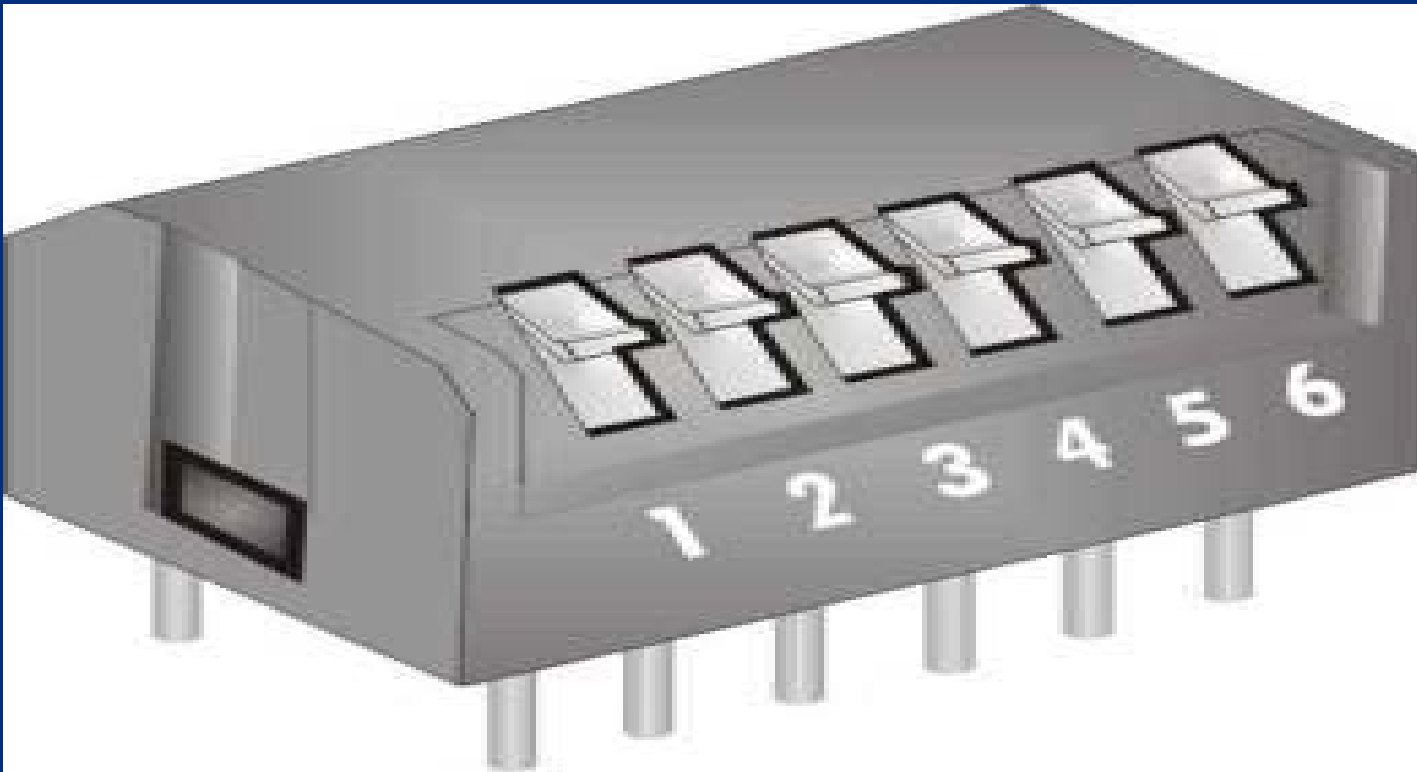
- *Dual Inline Package (DIP) switches* are small switches embedded into circuit boards
- Used to configure system functions including bus speed, processor speed and processor type
- Toggled either On/Off or 1/0
- Microsoft's standard Plug and Play feature made DIP switches obsolete



U.S. Department of
Homeland Security

United States
Secret Service

DIP Switch Example



*U.S. Department of
Homeland Security*

United States
Secret Service

Trusted Platform Module

- TPM is a microcontroller device installed on MB
- Stores encryption keys, passwords, and digital certificates
- Provides secure key generation that can be used to create and/or store both user and platform identity credentials for authentication
- Offers improved, hardware based security
- Uses RSA, and SHA-1 encryption algorithms



*U.S. Department of
Homeland Security*

United States
Secret Service

Power Supply

- Powers all internal components
- Come in different wattage models ranging from 63.5 to 1000-plus watts
- Each unit contains a power transformer that converts voltage from wall socket to power level computer can safely use
- Unit transmits a power good signal to MB
- Signal must be present continuously for computer to run or computer shuts down instantly



*U.S. Department of
Homeland Security*

United States
Secret Service

Power Supply

- Power good signal performs several functions:
 - Prevents computer from starting until appropriate level of operating voltage is reached
 - Interfaces with computer's reset switch
 - When reset switch is pressed, power good signal is grounded out
 - When reset switch is released, power good resumes and system reboots



*U.S. Department of
Homeland Security*

United States
Secret Service

ATX and AT Power Supplies

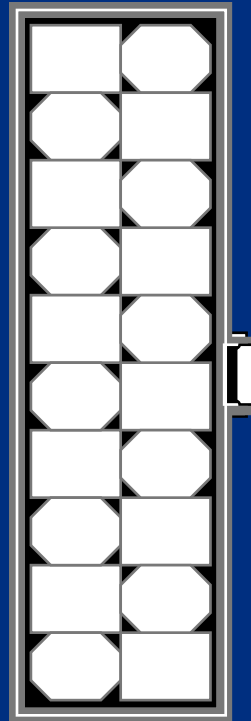
- Main plugs of ATX and AT power supplies are very different
- ATX has single, form-fitted plastic plug that fits into on-board socket that has unique configuration
- Plug is form fitted, will only fit into socket in one direction



*U.S. Department of
Homeland Security*

United States
Secret Service

ATX On-Board Power Socket (front view)



*U.S. Department of
Homeland Security*

United States
Secret Service

ATX and AT Power Supplies

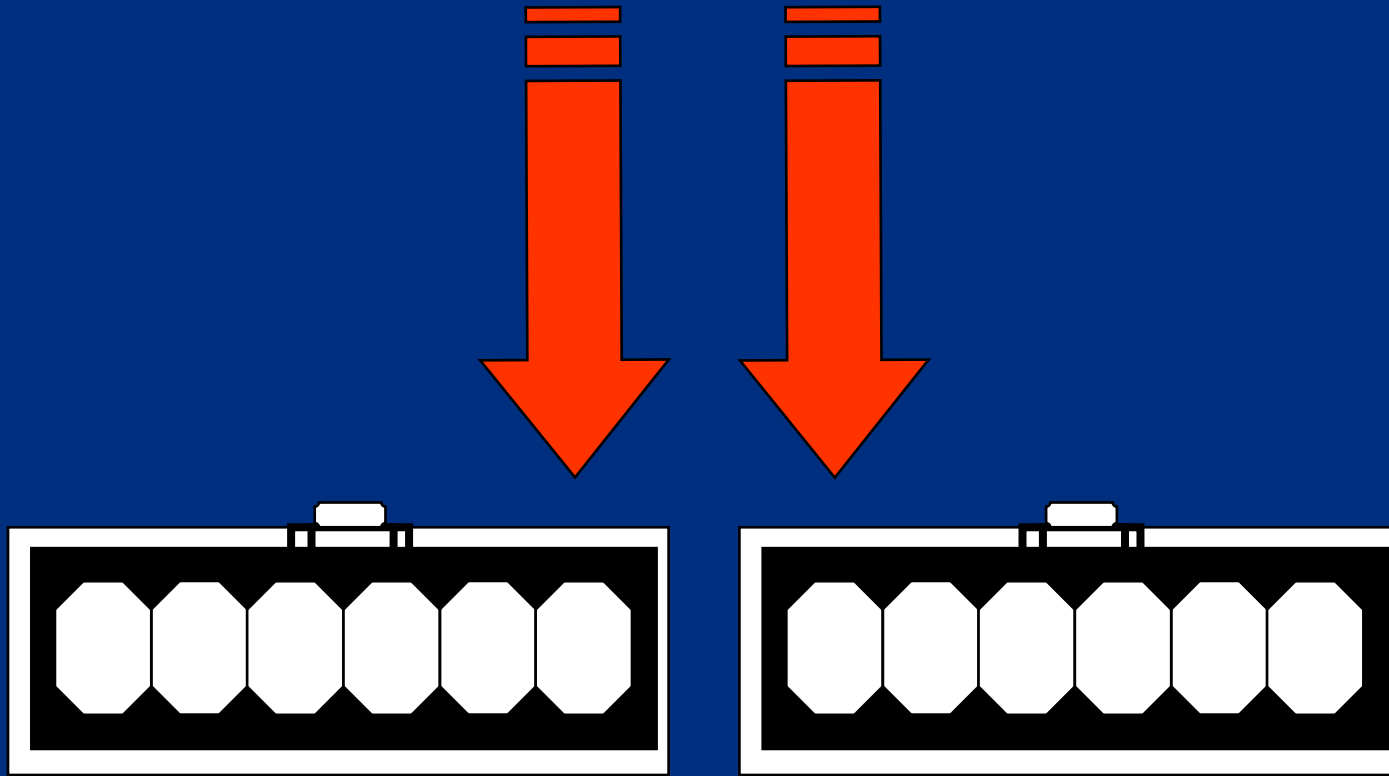
- In contrast, AT power supply has two separate plugs that fit into two separate on-board sockets
- Wires on plugs are color-coded
- Plugs are placed into sockets with black wires of both plugs located directly next to each other
- Properly connected, black wires will be in center of the two seated plugs



*U.S. Department of
Homeland Security*

United States
Secret Service

AT Power Connector Example



*U.S. Department of
Homeland Security*

United States
Secret Service

ATX and AT Power Supplies

- **Warning:** Unlike form-fitted ATX plug, AT plugs can be connected incorrectly. If AT plugs are not connected correctly, the motherboard will fail and fire may occur.



*U.S. Department of
Homeland Security*

United States
Secret Service

The Boot Process

- Predictable way a computer starts from moment Power On button is pressed until operating system loads



*U.S. Department of
Homeland Security*

United States
Secret Service

The Boot Process

Activity	Description
1. Power good signal is sent to CPU	When Power On button pressed
2. CPU looks at ROM for basic instructions (BIOS)	When CPU receives power good signal
3. System BIOS loads	
4. BIOS initiates POST	



*U.S. Department of
Homeland Security*

United States
Secret Service

The Boot Process

Activity	Description
5. POST checks RAM and Video. If either have a problem, there are various beep codes.	Typically, a procession of long single beeps for RAM; one long and two short for video.
From this point forward, errors are reported with text messages displayed on the monitor.	Motherboard documentation contains beep codes.



*U.S. Department of
Homeland Security*

United States
Secret Service

The Boot Process

Activity	Description
6. When RAM and Video pass POST test, single beep occurs. Single beep exists simply to indicate that diagnostic speaker is working. Malfunctioning speaker will prevent audible beep codes.	Begin to see text on screen. Rapid numbers flashing indicate an in-depth RAM check. Screen will indicate BIOS manufacturer and version number.



*U.S. Department of
Homeland Security*

United States
Secret Service

The Boot Process

Activity	Description
7. POST checks keyboard	If error occurs, text message generally displays on-screen
8. Legacy and then Plug and Play devices are identified	Data gathered is stored on CMOS chip



*U.S. Department of
Homeland Security*

United States
Secret Service

The Boot Process

Activity	Description
9. CMOS data queried against new current configuration data. Drives spin, lights flash, and sounds are heard.	If there is a problem with the CMOS battery, Text message explains.
10. Finding no major hardware errors, BIOS turns process over to boot loader.	



*U.S. Department of
Homeland Security*

United States
Secret Service

The Boot Process

Activity	Description
<p>11. The boot loader learns boot sequence (e.g. A: C: CD-ROM, etc.) and looks for Master Boot Record on device.</p> <p><i>For hard disks, the boot loader looks for a partition table. The partition table will have a pointer to the MBR on the primary, active partition</i></p>	



U.S. Department of
Homeland Security

United States
Secret Service

The Boot Process

Activity	Description
12. MBR contains first file needed to start operating system (IO.SYS in Windows 9x, boot.ini in NT).	
13. Process turned over to OS and you see splash screens, etc.	



*U.S. Department of
Homeland Security*

United States
Secret Service

Bus Overview

- Various buses comprise transportation system in computers
- Acts as a highway, sends data, signals, and power among processor, memory, and other components
- Two bus categories:
 - Internal bus connects all internal components to CPU and main memory
 - Expansion bus connects expansion boards to CPU and main memory



*U.S. Department of
Homeland Security*

United States
Secret Service

Bus Overview

- Key buses found in many computers include:
 - Processor bus
 - Memory bus
 - Accelerated Graphics Port (AGP) bus
 - Peripheral Component Interconnect (PCI) bus
 - PCI Express
 - Industry Standard Architecture (ISA) bus
 - Universal Serial bus (USB)
 - External SATA (E-SATA)



*U.S. Department of
Homeland Security*

United States
Secret Service

Bus Architecture

- Complex system of thin circuits known as *traces* that are located on any of several layers of MB
- System chipset orchestrates data transfer from all components via the bus
- Bus includes microchips and slots to hold expansion cards or circuit boards



U.S. Department of
Homeland Security

United States
Secret Service

Bus Architecture

- Buses are hierarchically arranged so each slower bus is connected to faster bus above
- Bus size, called width, describes amount of data (measured in bits) that can be transmitted at one time
- Bus's clock speed, measured in MHz, describes speed of data transfer



*U.S. Department of
Homeland Security*

United States
Secret Service

Processor and Memory Buses

- *Processor bus* is data pathway between CPU and MB chipset
- Also called front side bus, processor bus is fastest bus on MB
- Used by CPU to transfer information between cache or main memory and chipset
- *Memory bus* is data pathway between RAM and CPU, always same width as processor bus



U.S. Department of
Homeland Security

United States
Secret Service

ISA Bus

- Part of first IBM PC in 1984, 8 bits with speed of 5 MHz
- Today, ISA bus still remains slow at 16 bits and 8 MHz
- Ideal for slow-speed peripherals such as some older modems and sound cards
- Until recently, most MBs contained several ISA slots for backward compatibility
- Newer MBs have replaced ISA slots with PCI bus



*U.S. Department of
Homeland Security*

United States
Secret Service

Extended ISA Bus

- Extended ISA (EISA) bus is a 32-bit, non-proprietary slot connection designed to replace ISA bus
- Accepts ISA devices and has two slots
- Slots usually brown in color
- EISA bus now obsolete in PCs, still used in high-end servers



*U.S. Department of
Homeland Security*

United States
Secret Service

Micro Channel Architecture

- Micro Channel Architecture (MCA) connector was IBM proprietary slot connection designed to replace ISA/EISA cards
- MCA system now obsolete, may still be found in older IBM computer systems
- MCA introduced concept of *busmastering*
- Allows devices direct access to CPU via MB I/O controller for faster access
- Busmastering still used by modern devices



U.S. Department of
Homeland Security

United States
Secret Service

Micro Channel Architecture

- Two formats:
 - 16-bit with two slots
 - 32-bit with three slots (third slot is separated from other two)

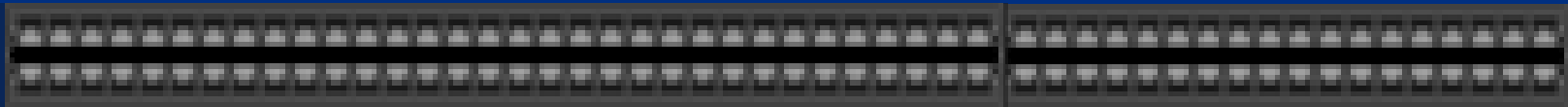


*U.S. Department of
Homeland Security*

United States
Secret Service

Micro Channel Architecture

MCA 16-bit bus (2 slots)



*U.S. Department of
Homeland Security*

United States
Secret Service

Micro Channel Architecture

MCA 32-bit bus (3 slots)



*U.S. Department of
Homeland Security*

United States
Secret Service

Video Electronic Standards Assoc. Local Bus

- The Video Electronic Standards Association (VESA) local bus (VL-Bus) is 32-bit, non-proprietary slot connection meant to replace ISA
- Has three slots (two together and one separated)
- First two slots (ISA) black, third slot brown, used for older video cards, replaced by PCI bus



*U.S. Department of
Homeland Security*

United States
Secret Service

PCI and PCI-X Bus

- *PCI bus*, collection of 32-bit or 64-bit connector slots on MB, generally white in color
- Modems, NICs, SCSI host adapters, and non-AGP video cards use PCI bus
- PCI local bus, also called mezzanine (meaning intermediary) bus because it sits in middle between CPU and RAM
- Part of North Bridge, can function with other devices and RAM without use of CPU



U.S. Department of
Homeland Security

United States
Secret Service

PCI and PCI-X Bus

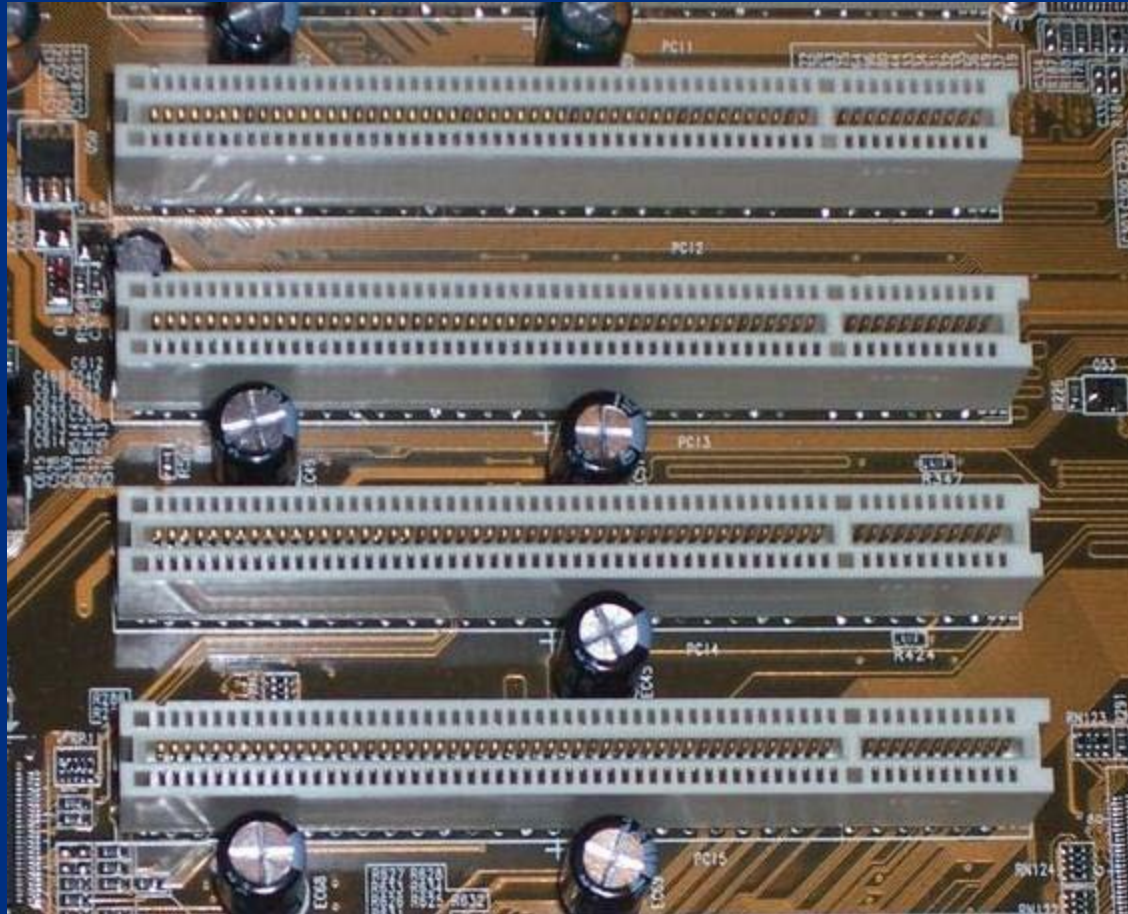
- PCI and PCI-X send data in parallel form in one direction at a time
- Speeds range from 33MHz (PCI) to 533MHz (PCI-X) with maximum of 34Gbits/sec transfer in most recent PCI-X
- All devices on a PCI bus take turns accessing bandwidth
- PCI-X completely backward compatible
- All 32-bit PCI cards function in PCI-X slot and new 64-bit PCI-X cards will function in standard PCI slot from late 1990s



*U.S. Department of
Homeland Security*

United States
Secret Service

Example of PCI and PCI-X Bus



*U.S. Department of
Homeland Security*

United States
Secret Service

PCI Express

- PCI advancement that sends data across lanes in serial form
- Capable of sending and receiving data simultaneously
- Various formats of PCI Express such as x1, x2, x4, x8, x12 and x16
- When multiplied by four, number represents number of lanes available to send and receive data
- Introduces lane switching, allows data to be switched along lanes as needed instead of devices taking turns waiting for bus



*U.S. Department of
Homeland Security*

United States
Secret Service

PCI Express

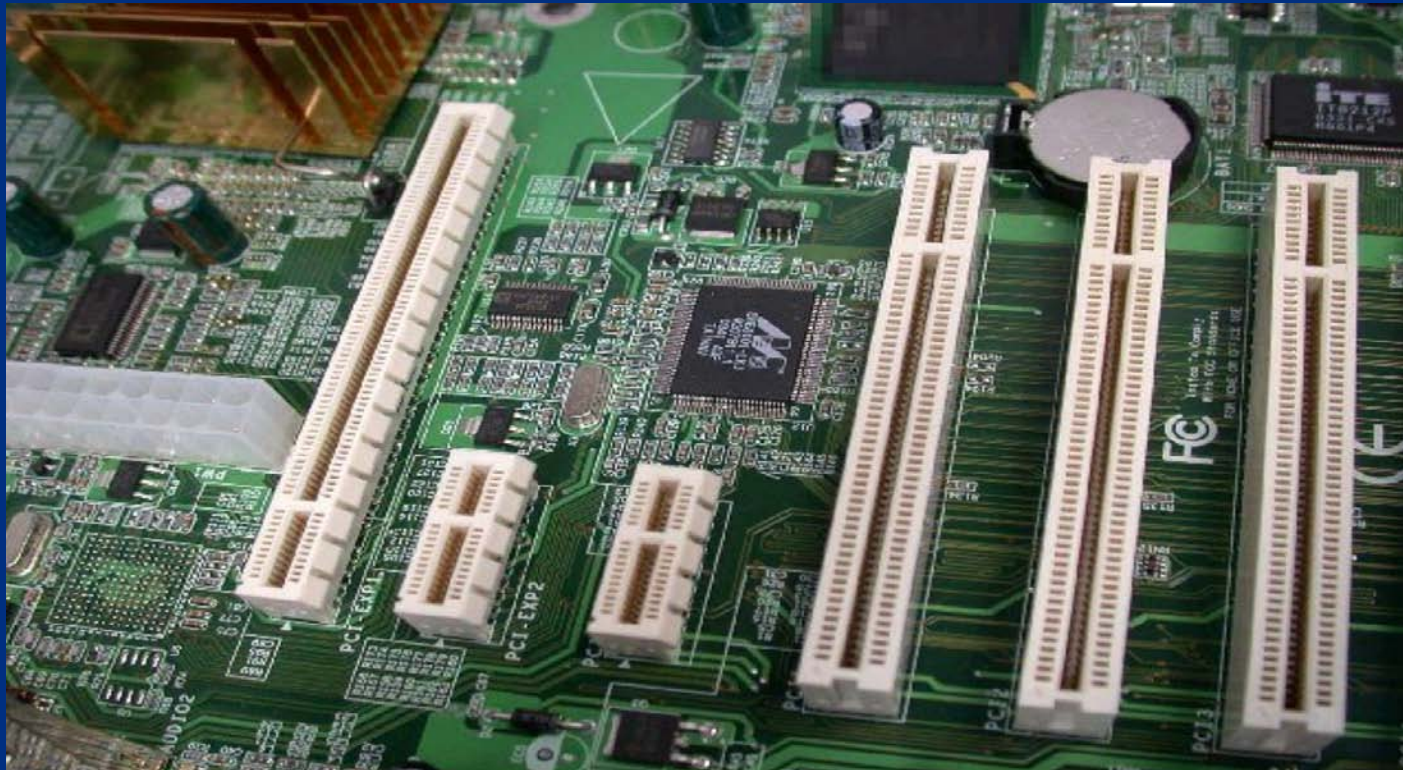
- PCI Express much more efficient than PCI or PCI-X
- Also known as 3GIO or 3rd generation input/output
- Most common formats are x1 and x2 for general peripheral devices and x16 as AGP replacement for graphics cards
- The x16 format can provide up to 128 Gb/sec throughput
- PCI Express connectors, generally black in color, physically different from PCI
- Not backward compatible with PCI or PCI-X



*U.S. Department of
Homeland Security*

United States
Secret Service

Example of PCI Express



U.S. Department of
Homeland Security

United States
Secret Service

AGP Bus

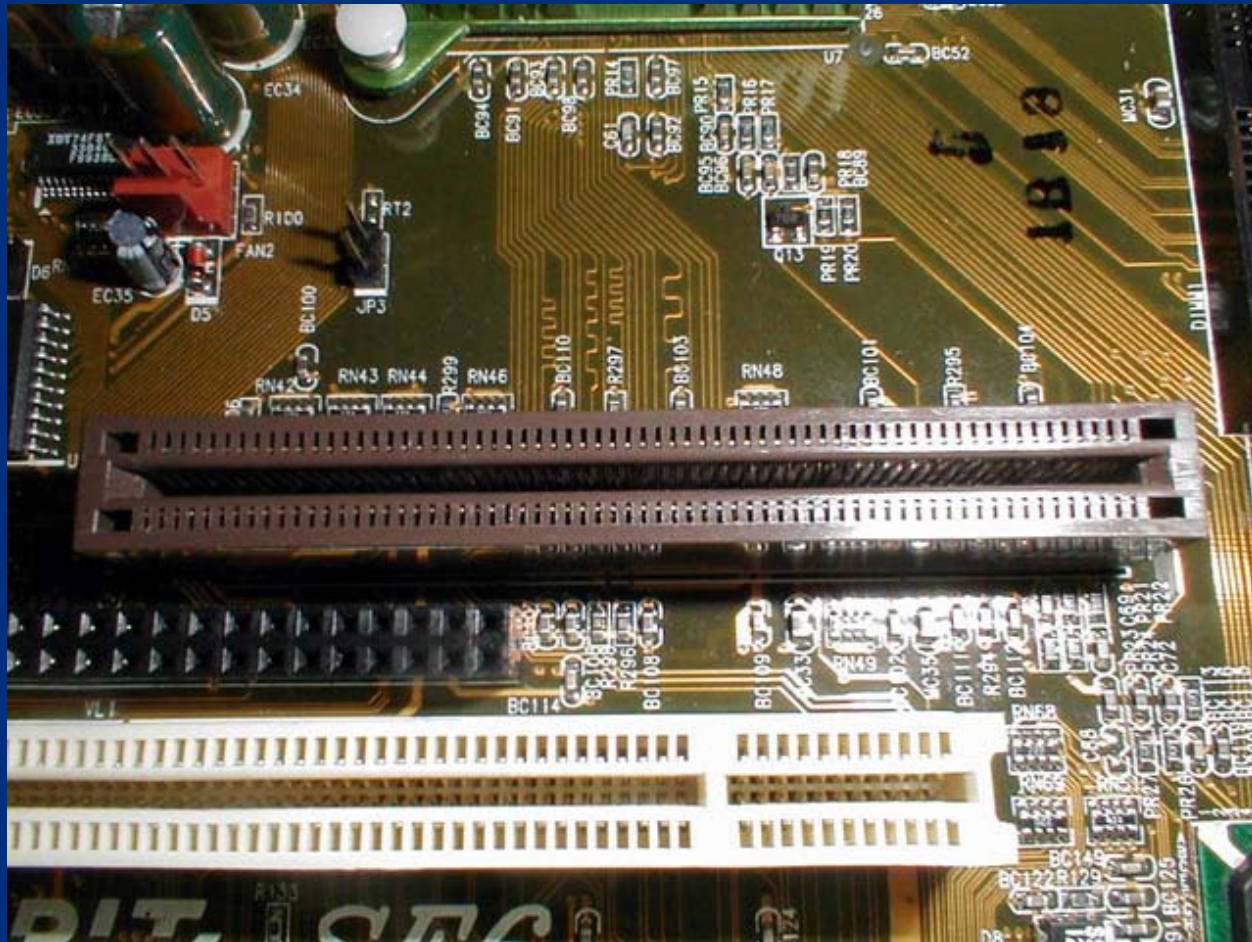
- Used exclusively for high-speed graphics processing
- This 66 MHz bus has a 32-bit slot connection, brown in color
- Reserved for a video card
- Available in 1x, 2x, 4x and 8x transfer rates
- AGP local bus placed near processor bus for direct access to it



*U.S. Department of
Homeland Security*

United States
Secret Service

Example of AGP Bus



U.S. Department of
Homeland Security

United States
Secret Service

USB

- Has port connection often located at rear of computer or on front panel
- Most computers have USB port used to connect various types of peripherals to system
- USB brings Plug and Play capabilities to peripherals connected outside PC
- Peripherals are automatically configured when attached to USB port, reboot is not necessary to use component



*U.S. Department of
Homeland Security*

United States
Secret Service

USB

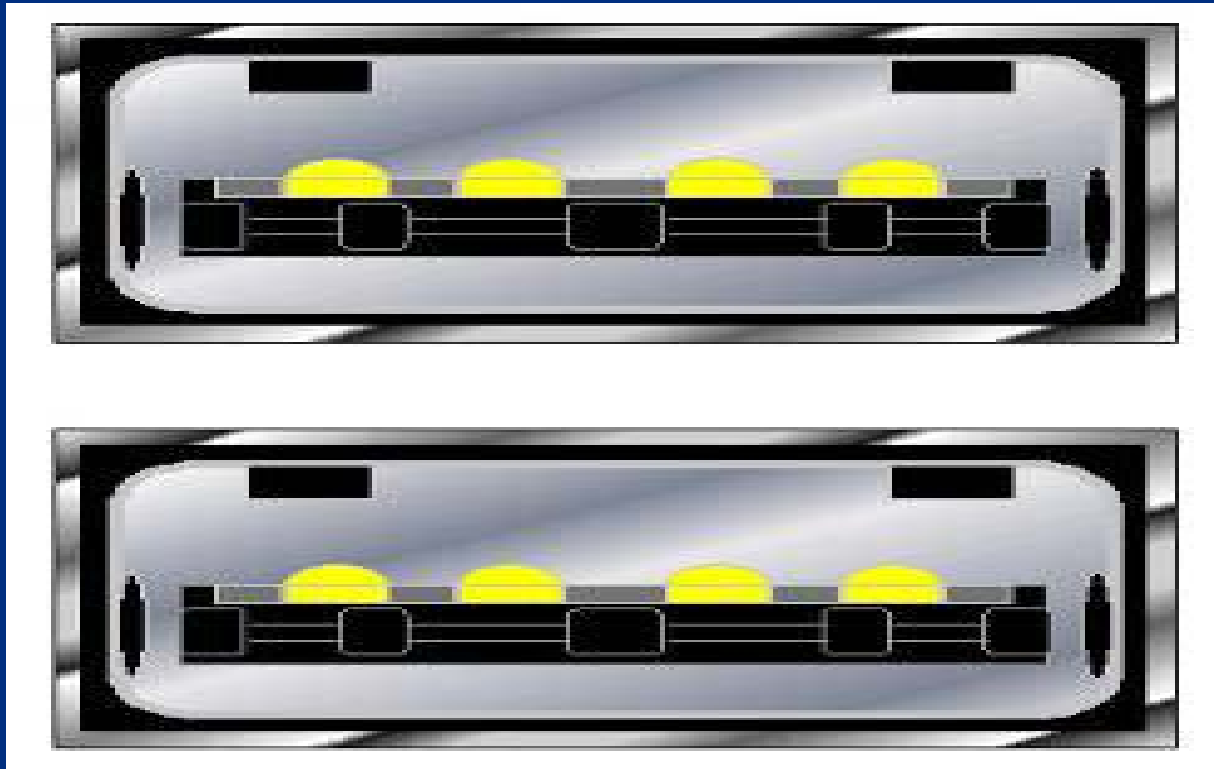
- USB specification, version 2.0, supports data transfer rate of 480 Mb/sec
- Version 2.0 backward compatible with earlier versions 1.1 and 1.0 that used 12 Mb/sec. and 1.5 Mb/sec. rates
- Continually evolving technology, evidenced by announcement of USB 3.0
- USB 3.0 increases speed rating of external devices by ten times that of USB 2.0, transferring data at 4.8 Gb/sec
- USB 3.0 will be fully compatible with 2.0 and 1.1 devices



*U.S. Department of
Homeland Security*

United States
Secret Service

Example of USB Ports



*U.S. Department of
Homeland Security*

United States
Secret Service

Wireless USB

- Along with wired USB solutions there are also recent innovations in Wireless USB (WUSB)
- WUSB allows for USB 2.0 speeds to devices within three meters of computer
- Works similar to Bluetooth, but features reduced range to support higher transfer speeds



*U.S. Department of
Homeland Security*

United States
Secret Service

IEEE 1394 (FireWire)

- IEEE 1394 is alternative to USB port
- FireWire by Apple and i.Link by Sony are two brands
- Allows 63 devices to be daisy chained to each connector
- Can handle multiple chains
- Transfer rate is approximately 400 Mb/sec, faster than USB 1.1 but slower than USB 2.0 480 Mb/sec
- 1394b standard allows faster signaling – up to 3.2 Gb/sec., requires special cables and interfaces



*U.S. Department of
Homeland Security*

United States
Secret Service

1394a (FireWire 400)

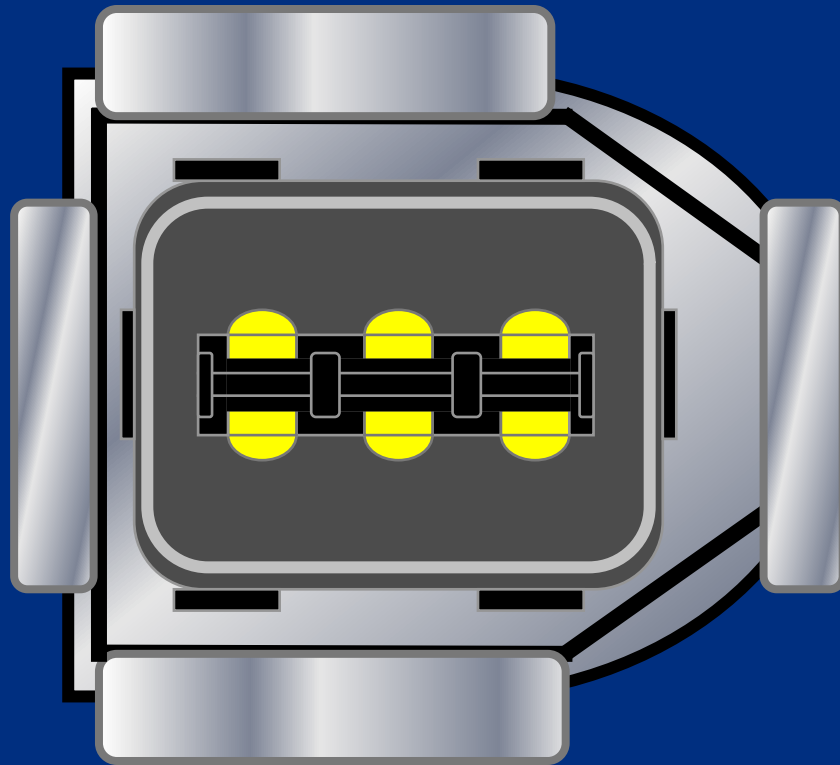
- 1394 and 1394a are original implementations of this bus type, with speeds up to 400 Mb/sec
- 1394a uses two styles of connectors: a 4-pin connector and a 6-pin connector
- The 6-pin has become a standard in many computers and external devices



*U.S. Department of
Homeland Security*

United States
Secret Service

IEEE 1394 Connector Example



*U.S. Department of
Homeland Security*

United States
Secret Service

1394b (FireWire 800)

- 1394b designed as higher performance bus type, allowing up to 800 Mb/sec and greater cable distances
- 1394b requires completely different cable and connector, a 9-pin connector
- Has not completely overtaken original 1394a
- Many modern devices feature both 1394a and 1394b connectors



*U.S. Department of
Homeland Security*

United States
Secret Service

Firewire S3200

- S3200 refers to a newer FireWire standard that uses existing 1394b cables to achieve data transfer rates of 3.2 Gb/sec, four times that of FireWire 800



*U.S. Department of
Homeland Security*

United States
Secret Service

E-SATA

- The E-SATA is an external port connection for external SATA devices, such as hard drives or DVD/CD devices
- E-SATA runs at speeds of 300 Mb/sec



*U.S. Department of
Homeland Security*

United States
Secret Service

Example of E-SATA Cable and Ports



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 4 - CPU and Memory

- CPU Functions
- Memory



*U.S. Department of
Homeland Security*

United States
Secret Service

CPU

- Computer's processor, most commonly called CPU or Central Processing Unit
- Main component that processes all software instructions and makes all calculations
- The CPU's main components are the following:
 - Arithmetic logic unit, handles all arithmetic and logical operations
 - Control unit, takes instructions from memory, translates them, and carries out instructions



*U.S. Department of
Homeland Security*

United States
Secret Service

CPU

- Either single-socket chip or chip mounted on a slot circuit board
- Various types from several manufacturers
- Each type connects to MB in different ways
- Some connect via socket in MB, others use a slot connector
- Each style is produced in variety of specific and unique designs, few compatible with each other



*U.S. Department of
Homeland Security*

United States
Secret Service

CPU

- CPU and MB must be completely compatible
- Socket-type CPUs, original method of producing CPUs, still most popular
- Actual CPU chip attaches to MB through a pin-grid array (PGA), a square receiver containing hundreds of evenly spaced holes
- Modern Intel CPUs designed as Plastic PGA (PPGA) or Flip-Chip PGA (FCPGA)



*U.S. Department of
Homeland Security*

United States
Secret Service

CPU

- Only physical difference between these is orientation of actual processor chip in relation to MB
- Late 1990's many CPUs designed using a slot-type connector
- Similar to PCI card, CPU would seat into a rectangular slot on MB
- Design was inefficient for faster clock speeds, phased out
- Pentium II, and many Pentium III processors designed as slot CPUs



*U.S. Department of
Homeland Security*

United States
Secret Service

Memory

- Temporary data storage area of a computer system
- System's workspace that houses programs and data being processed by CPU



*U.S. Department of
Homeland Security*

United States
Secret Service

Two main types of memory

- Read-only memory (ROM)
- Random access memory (RAM)



*U.S. Department of
Homeland Security*

United States
Secret Service

ROM

- Read-only memory (ROM), non-volatile, cannot be written to
- ROM chip contains MB BIOS used to boot system
- Four types of ROM chips:
 - ROM
 - Programmable ROM (PROM)
 - Erasable PROM (EPROM)
 - Electrically Erasable PROM (EEPROM) or FLASH ROM



*U.S. Department of
Homeland Security*

United States
Secret Service

ROM

- ROM – During manufacturing, binary data stored in die of silicon, cannot be changed without making new chip
- Programmable ROM (PROM) – Chip comes blank, needs to be programmed using special machine called device programmer, once PROM is written to, it cannot be changed



*U.S. Department of
Homeland Security*

United States
Secret Service

ROM

- Erasable PROM (EPROM) – Type of ROM that can be erased by exposure to high-intensity ultraviolet light, die used is sensitive to ultraviolet light, when exposed, all binary 0s changed back to 1s
- Electrically Erasable PROM (EEPROM) or FLASH ROM – Chips can be electrically erased and reprogrammed on circuit board using special software program, no other special equipment required to reprogram chip, modern MBs use this type chip for system board BIOS



*U.S. Department of
Homeland Security*

United States
Secret Service

RAM

- Random access memory (RAM), main memory, can be read by CPU and written to
- Temporary, relies on electrical power, also referred to as physical memory, actual chips that hold data
- Cleared when power is off or system reset
- RAM chips mounted on sticks that fit into slots on MB
- Slots arranged in numbered banks starting at 0
- Bank 0 is usually located nearest CPU



*U.S. Department of
Homeland Security*

United States
Secret Service

Dynamic RAM (DRAM)

- Most common and least expensive memory chip, small with high data density (up to 256K)
- Several DRAM chips mounted on a single stick that fits into connection slots on MB
- Connection slots are arranged in banks starting at 0



*U.S. Department of
Homeland Security*

United States
Secret Service

Dynamic RAM (DRAM)

- Bank 0 is usually located nearest CPU
- Requires constant electrical refreshing to keep it dynamic
- Uses capacitors and transistors in pairs, capacitors hold charges (both positive and negative) that indicate whether transistor is On or Off, charge holds power in transistor and keeps RAM contents alive



*U.S. Department of
Homeland Security*

United States
Secret Service

SIMM (Single Inline Memory Modules)

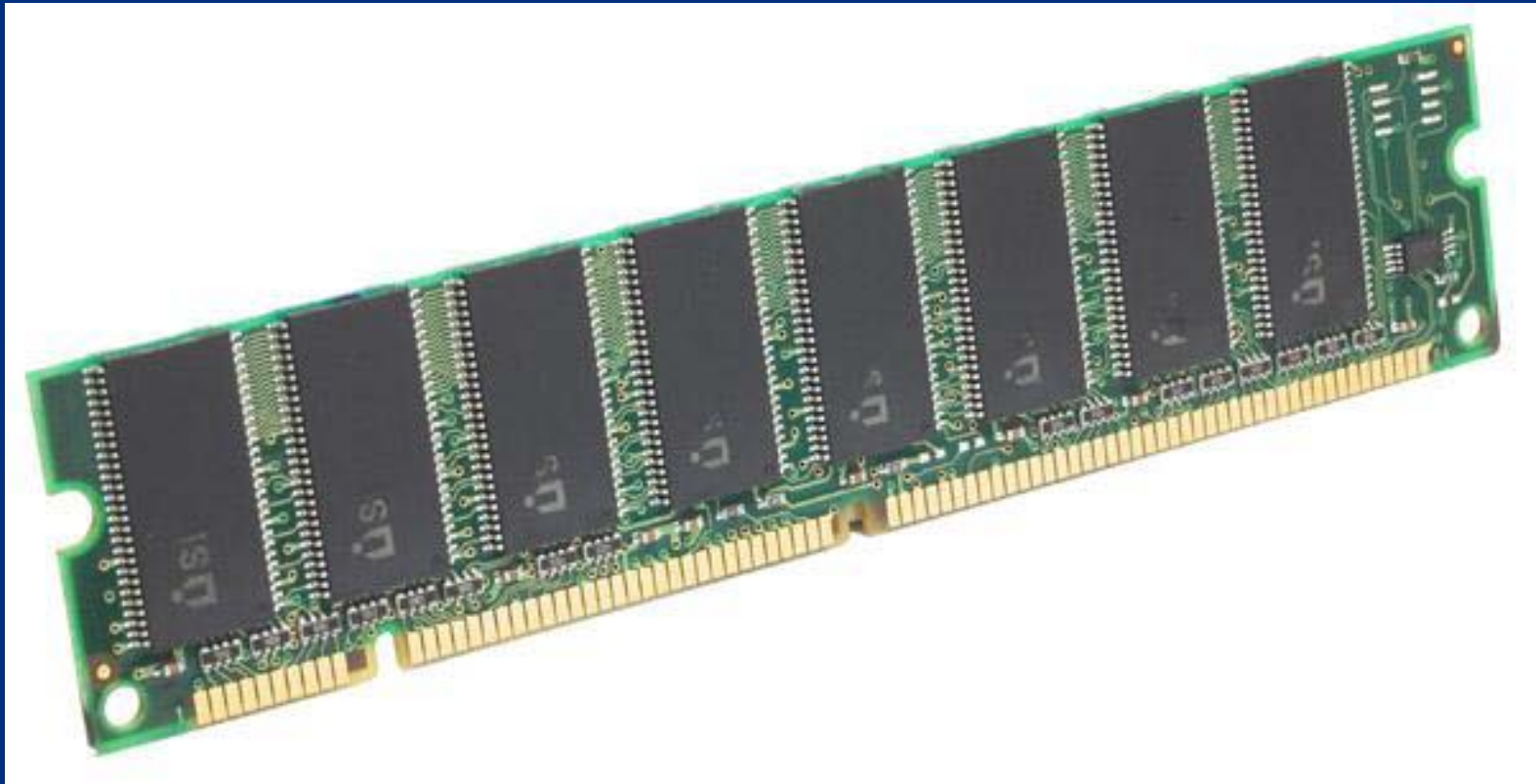
- Used in earlier generation PCs, manufactured in sizes ranging from 512 KB to 32 MB, with flat connection pins in two types:
- 30-pin SIMM, considered obsolete in PCs (used with 386 processors and below), installed in pairs
- 72-pin SIMM, still available, installed singularly on MBs with CPUs below Pentiums, in pairs on Pentiums and above, widely used a few years ago until replaced by DIMMs



*U.S. Department of
Homeland Security*

United States
Secret Service

Example of SIMM Chip



*U.S. Department of
Homeland Security*

United States
Secret Service

DIMM (Dual Inline Memory Modules)

- Most widely used memory modules, 168-pin DIMMs, which have replaced SIMMs
- 64 bits wide, range in size from 8 MB to 1 GB
- DIMMS, inserted straight into sockets and locked in place



*U.S. Department of
Homeland Security*

United States
Secret Service

Synchronous DRAM (SDRAM)

- SDRAM is modern memory standard, faster than regular DRAM
- Most prevalent in Pentium II/Athlon systems and above
- Runs in synchronization with actions of processor bus
- Performs operation at same time as system clock and at same speed, increases speed of data input/output
- All SDRAM are DIMMs
- All DIMMs not necessarily SDRAM



*U.S. Department of
Homeland Security*

United States
Secret Service

Synchronous DRAM (SDRAM)

- SDRAM is manufactured at single, double data rate, or quad data rate (SDR, DDR, DDR2 and DDR3)
- Rates describe speed of data transfer per clock cycle
- There are several SDRAM speeds
- Type and speed system requires depends on MB



*U.S. Department of
Homeland Security*

United States
Secret Service

Synchronous DRAM (SDRAM)

- When upgrading SDRAM, select speeds greater than or equal to frontside (processor) bus speed
- Pushing slower RAM at higher speeds (overclocking) will cause RAM to overheat and malfunction
- Can cause permanent damage to MB
- Acceptable to install faster RAM into slower MB
- SDRAM is *not* compatible with all MBs, refer to MB documentation



U.S. Department of
Homeland Security

United States
Secret Service

RIMM (RAMBUS Inline Memory Modules)

- RIMMs are found in high-end computers
- Offer highest performance of available memory
- Capable of transfer speeds of over 6 GB/s
- Memory modules use RAMBUS Dynamic RAM (RDRAM) chips, a proprietary chip format
- Generally geared towards server market although Intel actively pushed technology towards consumer market
- Due to high cost, uncommon on most computers



*U.S. Department of
Homeland Security*

United States
Secret Service

RIMM (RAMBUS Inline Memory Modules)

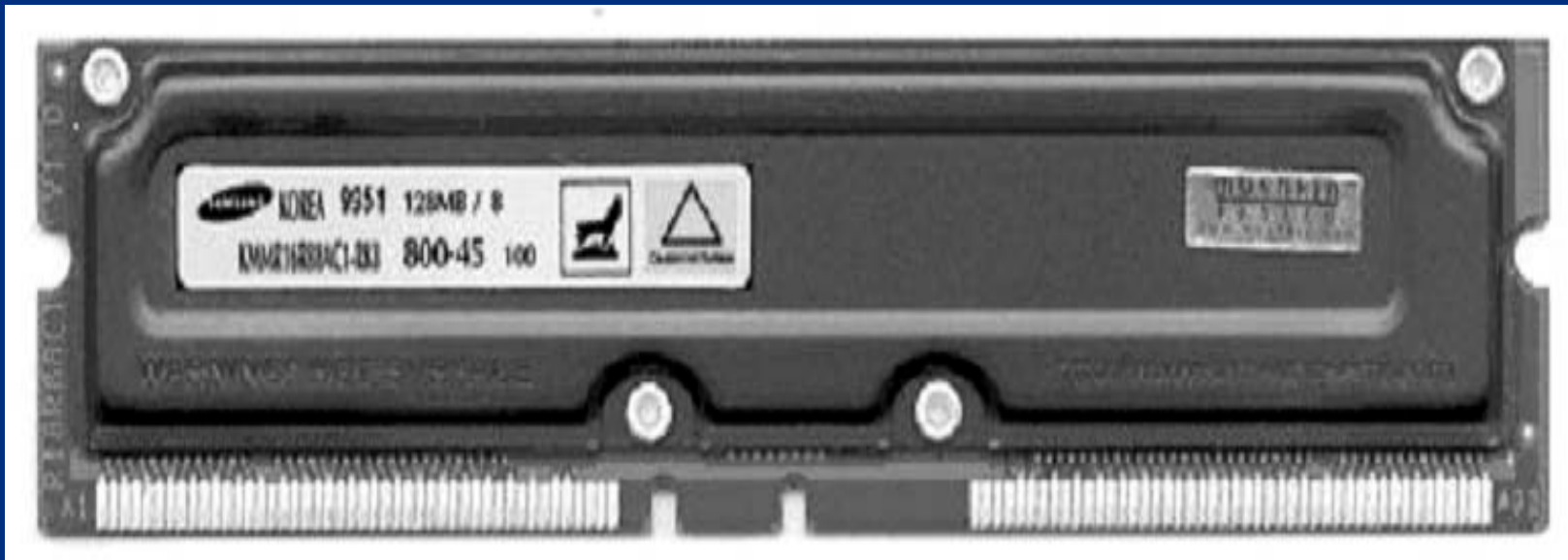
- RIMMS manufactured with 184 connection pins
- Sizes range from 64 MB to 1 GB
- Most MBs require RIMM chips be installed in pairs
- If only single memory module needed, a special continuity unit (CU) is required to provide termination
- CUs are additional RIMM modules without RDRAM chips that are plugged into remaining RIMM slots not occupied by memory modules



*U.S. Department of
Homeland Security*

United States
Secret Service

Example of RIMM Chip



*U.S. Department of
Homeland Security*

United States
Secret Service



*U.S. Department of
Homeland Security*

United States
Secret Service

Data Storage Components



*U.S. Department of
Homeland Security*

United States
Secret Service

You will learn ...

- Hard Disk Drives
- Floppy Drives and Removable Media



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 1 - Hard Disk Drives

- Hard Drive Components
- Hard Drive Controllers
- Hard Drive Geometry
- Drive Preparation - Wiping
- RAID Configuration Overview



*U.S. Department of
Homeland Security*

United States
Secret Service

Saving a File to a Hard Drive

- As file is written or created, contents temporarily stored in RAM
- To save file, operating system takes file from RAM and stores permanently to hard drive
- Saving file initiates complex process that records the file and tracks storage location on hard drive



*U.S. Department of
Homeland Security*

United States
Secret Service

Process for Storing Data on Hard Drive

Step	Activity
1	User makes request to save file. File is temporarily stored in RAM (if not already residing there).
2	File system analyzes disk to find required available space.
3	Operating system receives request to transfer file from RAM to permanent storage on disk.



*U.S. Department of
Homeland Security*

United States
Secret Service

Process for Storing Data on Hard Drive

Step	Activity
4	File system (FAT, VFAT, FAT32, NTFS, ext2 or ext3) updates file directory with newly saved file name and exact location or directory path.
5	Operating system tells drive controller to save file. File then transferred from RAM to hard drive.
6	Once saved, file system marks area of disk as not available. Area cannot be overwritten by subsequent file saves.



*U.S. Department of
Homeland Security*

United States
Secret Service

Hard Drive Components

- Disk platters
- Read/write heads
- Head actuator
- Spindle motor
- Jumpers and/or switches
- Disk controller
- Cables and connections



*U.S. Department of
Homeland Security*

United States
Secret Service

Disk Platters

- Hard drive stores archival copies of data on non-volatile disk platters made of metal or glass with magnetic medium coating
- Most hard drives can hold several 3.5-inch platters with capacity of 250 GB or higher
- Laptops and notebook computers use 2.5-inch platters with capacity of 100 GB each
- Data stored on both sides of each disk platter



*U.S. Department of
Homeland Security*

United States
Secret Service

Disk Platters

- In operation, disk spins as read/write heads move over disks and store information in tracks and sectors
- Data is stored in concentric rings or tracks on disks
- Tracks are divided into segments called sectors
- Each sector can store approximately 512 bytes of data



*U.S. Department of
Homeland Security*

United States
Secret Service

Read-Write Heads

- Mechanisms that store and read data on platters
- One read-write head combination for each side of disk platter, all heads mounted on a single track
- Move in unison across platters
- Float above surface of disk platter on cushion of air generated by action of spinning disk platter



*U.S. Department of
Homeland Security*

United States
Secret Service

Read-Write Heads

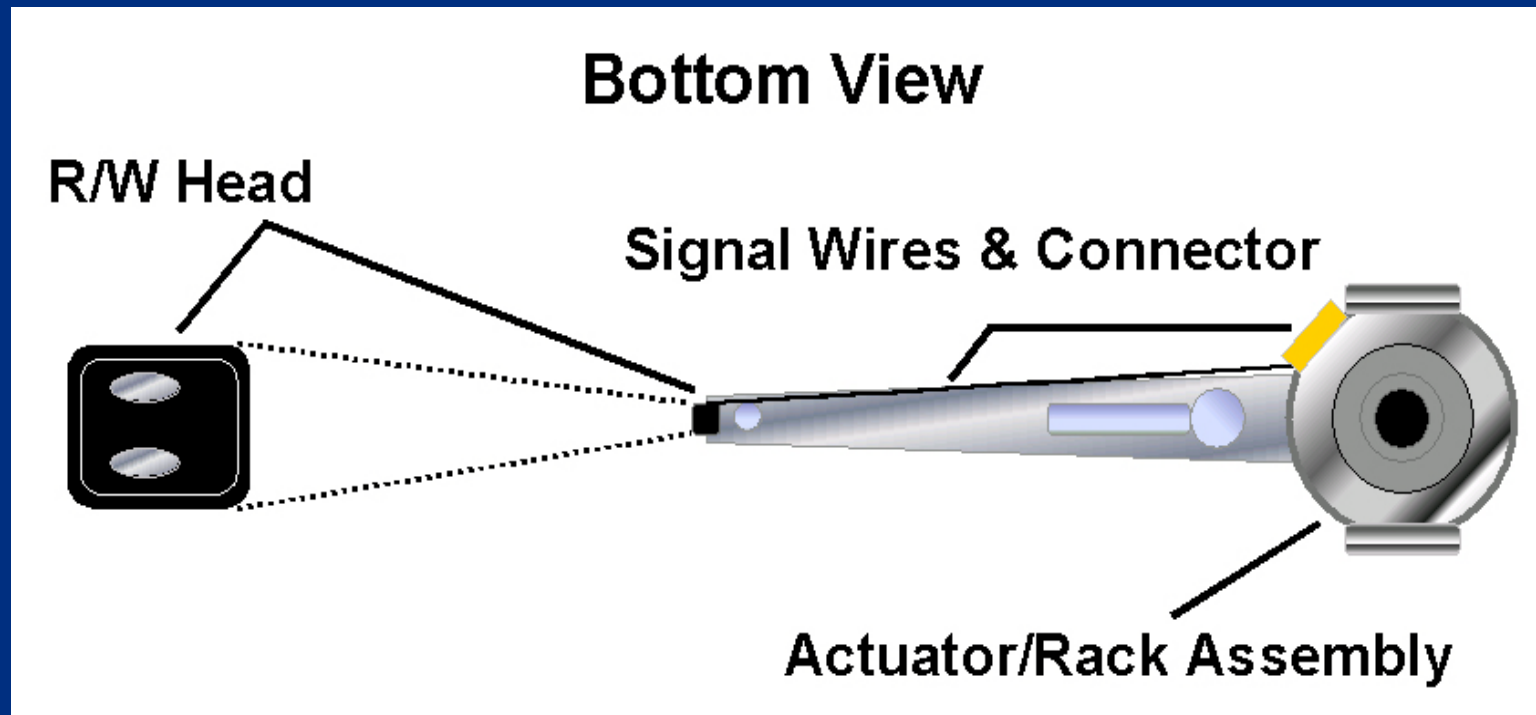
- Float three to five millionths of an inch above platters
- Read changes in disk's magnetic coating, called magnetic flux
- Data is stored on both sides of platters
- Side numbering starts at zero for top side of top platter
- For example, if drive has four platters (eight sides), numbering for sides would be zero through seven



*U.S. Department of
Homeland Security*

United States
Secret Service

Read-Write Heads



*U.S. Department of
Homeland Security*

United States
Secret Service

Jumpers

- Set of pins used to control device settings
- Pins act like an on/off switch and are configured by placement of a small plastic block, called a shunt
- Without shunt over jumper pins, circuit is open, or off
- With shunt placed over pins, small wire inside shunt connects pins and circuit is closed, or on, also called shorted



*U.S. Department of
Homeland Security*

United States
Secret Service

Jumpers

- Shunt can also be attached to a single pin in parked position, does not close circuit, simply used to store shunts not currently needed
- Jumpers used when installing PATA (Parallel ATA) IDE devices
- Typical MBs house two PATA IDE channels identified by a Primary (IDE 1) Connector and a Secondary (IDE 2) Connector



*U.S. Department of
Homeland Security*

United States
Secret Service

Jumpers

- Each IDE channel can support maximum of two IDE devices
- Relationship of two devices on a single channel is master and slave, simply designates sequential order of devices



*U.S. Department of
Homeland Security*

United States
Secret Service

Four IDE Device Relationships

- Primary Master: Device 1 on primary IDE 1 channel
- Primary Slave: Device 2 on primary IDE 1 channel
- Secondary Master: Device 1 on secondary IDE 2 channel
- Secondary Slave: Device 2 on secondary IDE 2 channel



*U.S. Department of
Homeland Security*

United States
Secret Service

Jumpers

- Designation of master and slave between two devices on same IDE channel determined by jumper settings on IDE devices
- Drives normally contain diagram indicating which pins to short and which to leave open



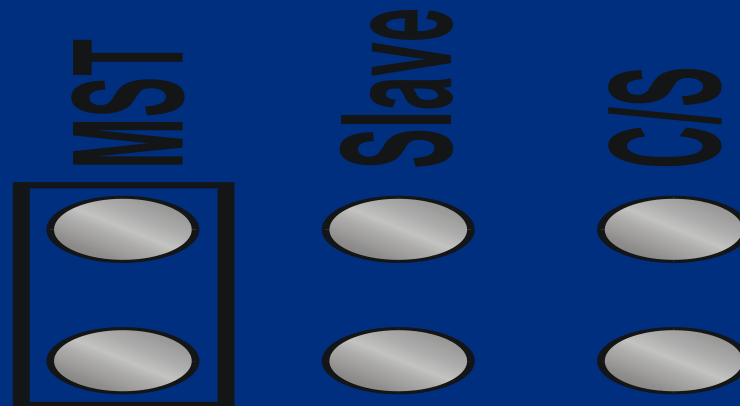
*U.S. Department of
Homeland Security*

United States
Secret Service

Setting the Master Drive

To indicate a primary hard drive in a series of two, close Master jumper as in the following configuration

Master

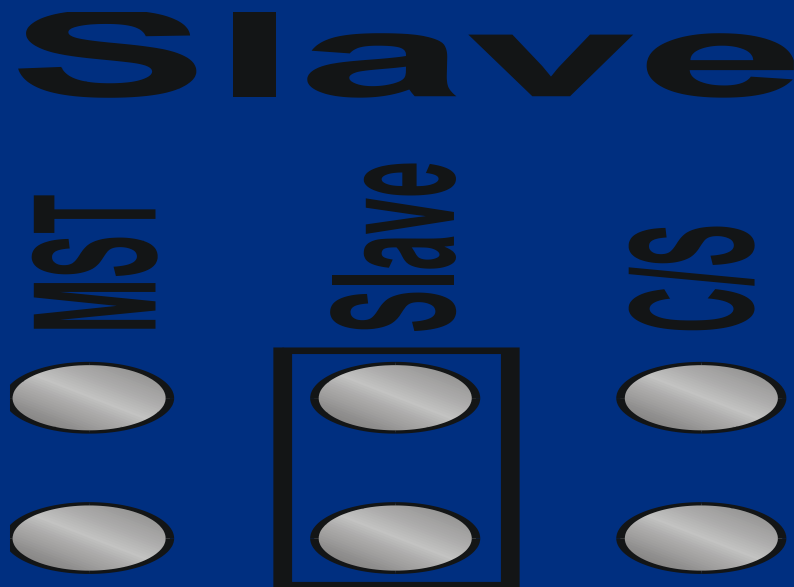


*U.S. Department of
Homeland Security*

United States
Secret Service

Setting the Slave Drive

To indicate a secondary hard drive in a series of two, close the Slave jumper as in the following configuration



*U.S. Department of
Homeland Security*

United States
Secret Service

Jumpers

- On newer MBs, with support for SATA (Serial ATA) devices, MB may have only one PATA connector or none
- SATA devices do not require a jumper for Master and Slave settings
- SATA device plugged onto its own MB connector



*U.S. Department of
Homeland Security*

United States
Secret Service

PATA Data Cables

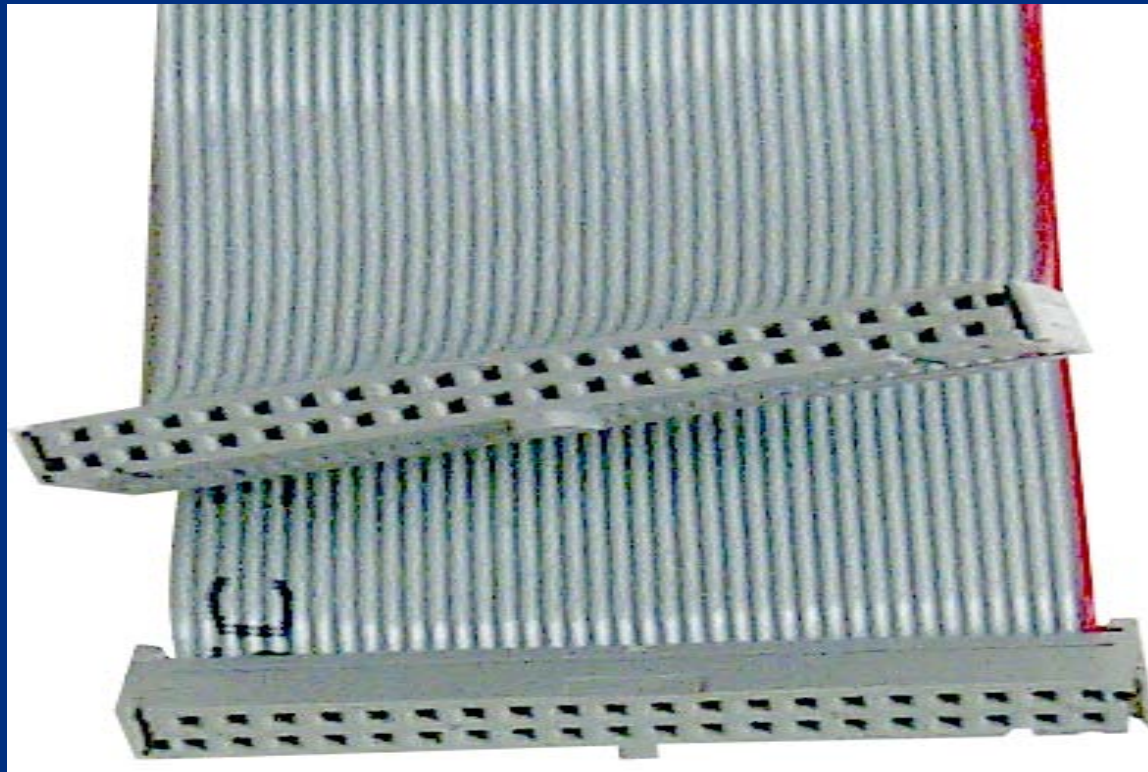
- Older PATA IDE hard drives, and CD-ROMs, connect to MB via a ribbon cable to facilitate data transfer
- Cables are flat and wide with wires running in parallel the length of cable
- IDE ribbon cables generally have three 40-pin connectors: one to attach to MB and one each for Master and Slave device
- A red or black stripe along one edge of the cable indicates location of Pin 1 and is used to determine cable orientation



*U.S. Department of
Homeland Security*

United States
Secret Service

40-pin Ribbon Cable



*U.S. Department of
Homeland Security*

United States
Secret Service

SATA Data Cables

- SATA (Serial ATA) is a communication bus technology that is replacing older PATA (IDE) technology
- SATA does not use Master/Slave jumpers on hardware to determine device priorities
- SATA device has its own dedicated connection to host device



*U.S. Department of
Homeland Security*

United States
Secret Service

SATA Data Cables

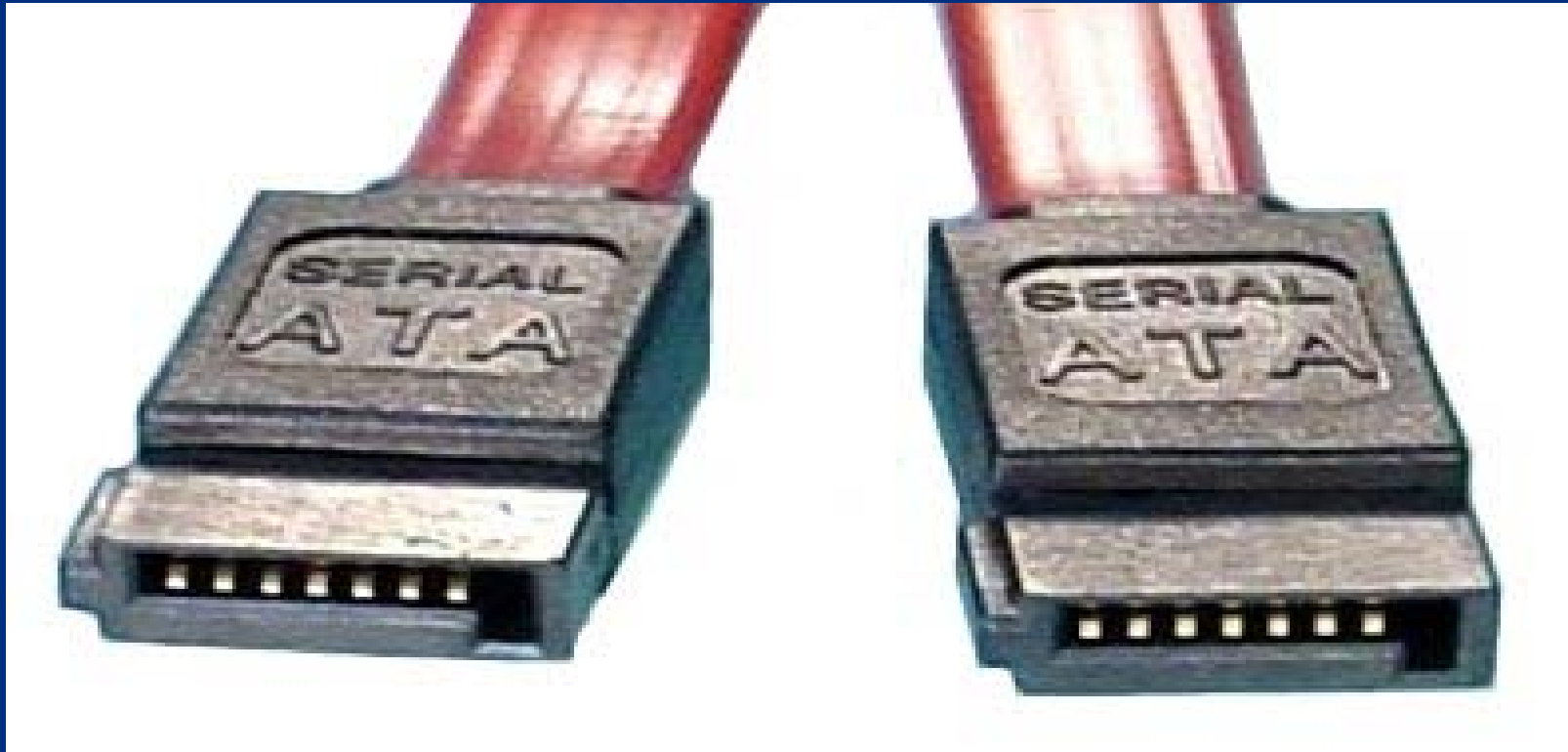
- Bandwidth is not shared with other devices over SATA data cables
- SATA offers other benefits over PATA, such as more compact cables for better airflow and hot swapping capabilities
- SATA data cables use 7-pin connectors that only utilize 4 wires for transferring data.
- Other 3 wires used as ground



*U.S. Department of
Homeland Security*

United States
Secret Service

SATA Data Cable



*U.S. Department of
Homeland Security*

United States
Secret Service

SATA Power Cables

- New power connector also specified by SATA standard, although many SATA devices include both SATA and Molex power connectors
- Cable designed with 15-pins and supports three different voltages; 3.3 V, 5 V, and 12 V
- Nine of 15 pins used for power, 5 used for ground, and last pin used for staggered spinup
- Staggered spinup allows drives to initialize and power up sequentially to increase reliability and prevent power surges



*U.S. Department of
Homeland Security*

United States
Secret Service

SATA Power Cable



*U.S. Department of
Homeland Security*

United States
Secret Service

Drive Controllers

- Device that handles transfer of data between component and computer
- Required by computer storage devices including hard drives and floppy drives to govern how they operate



*U.S. Department of
Homeland Security*

United States
Secret Service

Drive Controllers

- Disk drive controllers discussed in this course include:
 - Integrated Drive Electronics (IDE)
 - Enhanced IDE (EIDE)
 - Serial ATA (SATA)
 - Small Computer System Interface (SCSI)
 - Serial Attached SCSI (SAS)



*U.S. Department of
Homeland Security*

United States
Secret Service

Integrated Drive Electronics (IDE) Controller

- Term used to describe any disk drive with a built-in controller
- Technical name for IDE is Advanced Technology Attachment (ATA) IDE
- IDE is primary interface electronics (controller) that connects a hard disk drive to computer



*U.S. Department of
Homeland Security*

United States
Secret Service

Integrated Drive Electronics (IDE) Controller

- Today's technology allows IDE to be integrated into the drive
- Drive attaches to a connector on MB
- IDE makes drive more reliable than drives that have separate ISA slotted controllers
- Reliability enhances integrity of data



*U.S. Department of
Homeland Security*

United States
Secret Service

Integrated Drive Electronics (IDE) Controller

- IDE controllers are customized to fit IDE drives
- IDE controllers contain an independent BIOS that limits total hard drive size to 528 MB
- Uses a standard 40-pin ribbon cable to connect drive to MB

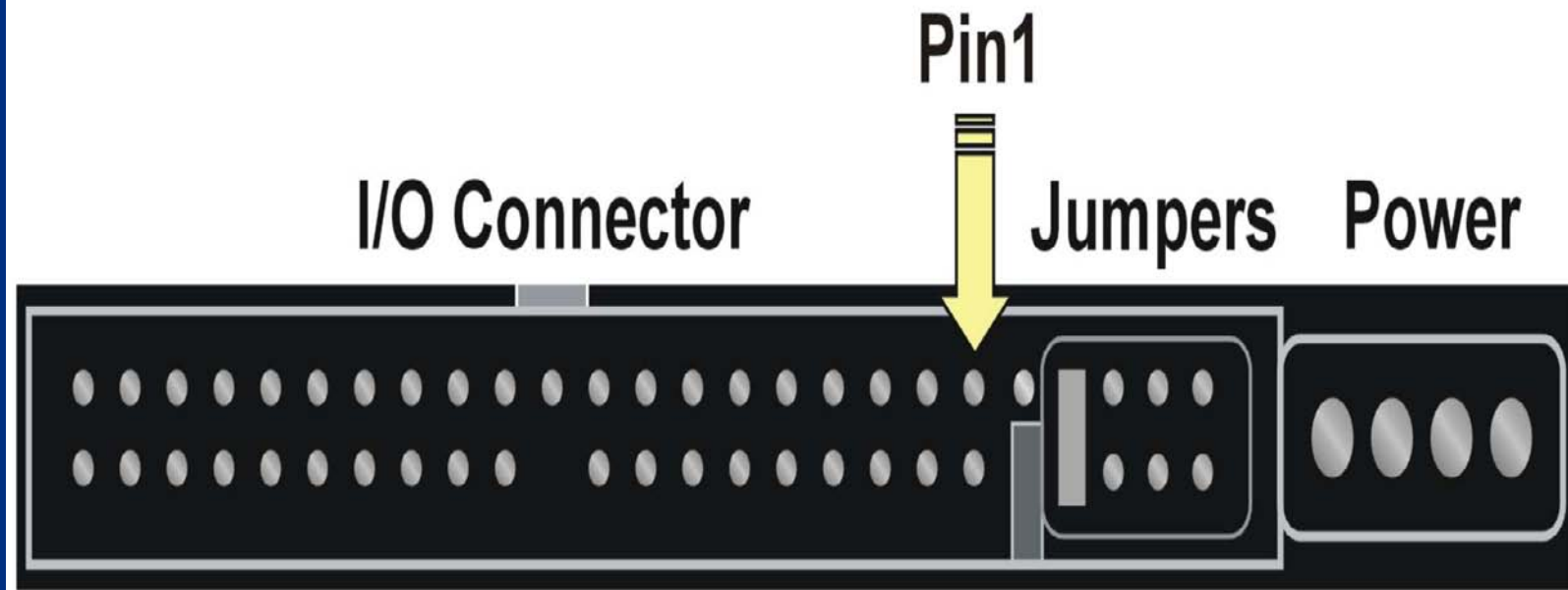


*U.S. Department of
Homeland Security*

United States
Secret Service

IDE Controller Connection

Rear View



*U.S. Department of
Homeland Security*

United States
Secret Service

Enhanced IDE Controller

- Enhanced IDE (EIDE) controllers offer enhanced controller BIOS, increases maximum drive capacity to more than 528 MB
- Controller's technical names are Advanced Technology Attachment series ATA-2 through ATA-6
- Marketed as Fast ATA and Fast ATA2, drives are backward compatible with older models



*U.S. Department of
Homeland Security*

United States
Secret Service

Enhanced IDE Controller

- EIDE provides two data channels per connector, two drives can be connected to each EIDE port
- EIDE allows attachment of Advance Technology Attachment Packet Interface (ATAPI) devices, CD-ROM drives, DVD drives, and Zip drives



*U.S. Department of
Homeland Security*

United States
Secret Service

Enhanced IDE Controller

- ATA-1, 2, and 3 Controllers:
 - Use CPU for data transfer (PIO mode) which takes CPU transferring time away from other tasks
 - ATA-1 support a transfer rate of up to 8 MB/sec
 - ATA-2 support a transfer rate of up to 16 MB/sec
 - ATA-3 support a transfer rate of up to 16 MB/sec



*U.S. Department of
Homeland Security*

United States
Secret Service

Enhanced IDE Controller

- ATA-4, 5 and 6 Controllers:
 - Use Direct Memory Addressing (DMA) modes for data transfer
 - ATA-4 support a transfer rate of up to 33 MB/sec
 - ATA-5 supports transfer rates of up to 66 MB/sec
 - ATA-6 supports transfers rates of up to 100 MB/sec
 - To achieve rates of speed of 66 MB/sec or more, a special 40-pin, 80-wire ribbon cable must connect hard drive to MB



*U.S. Department of
Homeland Security*

United States
Secret Service

PATA Naming Convention

- While ATA, IDE, and EIDE technically refer to three separate concepts, they are generally grouped together and referred to as the same technology
- Often terms are used interchangeably to refer to hard drives with exceptions of SCSI and SATA
- Since introduction of SATA (Serial ATA), all examples of prior hard drives have been retroactively renamed to PATA (Parallel ATA)



*U.S. Department of
Homeland Security*

United States
Secret Service

Serial ATA (SATA)

- Two-inch wide parallel PATA ribbon cable has reached maximum transfer rate of 133 MBps
- SATA currently has speeds of 150 MBps (SATA 1.5G) and 300 MBps (SATA 3G) and potential to reach 600 MBps (SATA 6G)
- Serial ATA's power requirements, 250 millivolt versus PATA's 5 volt, have made it widely adopted in new low-power MBs



*U.S. Department of
Homeland Security*

United States
Secret Service

Serial ATA (SATA)

- Serial ATA drives connect via a .25-inch cable that connects drive to Serial ATA card plugged into a PCI slot or a slot integrated onto MB
- SATA cables have seven pins and seven wires
- Thinner cables permit better airflow, smaller, easier to route
- Parallel ATA cables are two inches wide and have maximum length limitation of 18 inches
- SATA cable has maximum length limitation of one meter



*U.S. Department of
Homeland Security*

United States
Secret Service

Serial ATA (SATA)

- Each SATA connection supports a single drive
- Jumpers settings no longer required for master or slave configuration
- SATA allows hot swapping of drives while system is running



*U.S. Department of
Homeland Security*

United States
Secret Service

Serial ATA (SATA)

- External SATA connection allows for SATA drives to be connected externally with transfer speeds up to 300 MBps, six times faster than USB 2.0
- The eSATA shielded cables are found in lengths up to two meters but do not provide power to end device
- eSATA currently geared towards external SATA hard drives but able to accommodate large variety of external devices, including CD-ROMs



*U.S. Department of
Homeland Security*

United States
Secret Service

Small Computer System Interface (SCSI)

- System level interface that enables connection of various peripheral devices to computer
- Most modern home PCs do not come with SCSI hardware preinstalled
- Any computer with a PCI slot can become SCSI compatible



*U.S. Department of
Homeland Security*

United States
Secret Service

Small Computer System Interface (SCSI)

- SCSI is not a controller like IDE
- Separate data bus that connects to system bus via a host adapter
- Some high-end computers have a SCSI adapter card or an adapter built into MB
- Some current SCSI busses can support between 8 and 16 devices, though support for one device is lost to host adapter



*U.S. Department of
Homeland Security*

United States
Secret Service

Small Computer System Interface (SCSI)

- SCSI implementations can support many more devices, such as SSA which supported 96 and SAS (Serial Attached SCSI) which supports 16,256
- Devices are strung together in a chain, each device is assigned a SCSI ID
- Typical SCSI host adapter can support a maximum of 16 devices, though actual SCSI adapter counts as one of those 16 devices



*U.S. Department of
Homeland Security*

United States
Secret Service

Small Computer System Interface (SCSI)

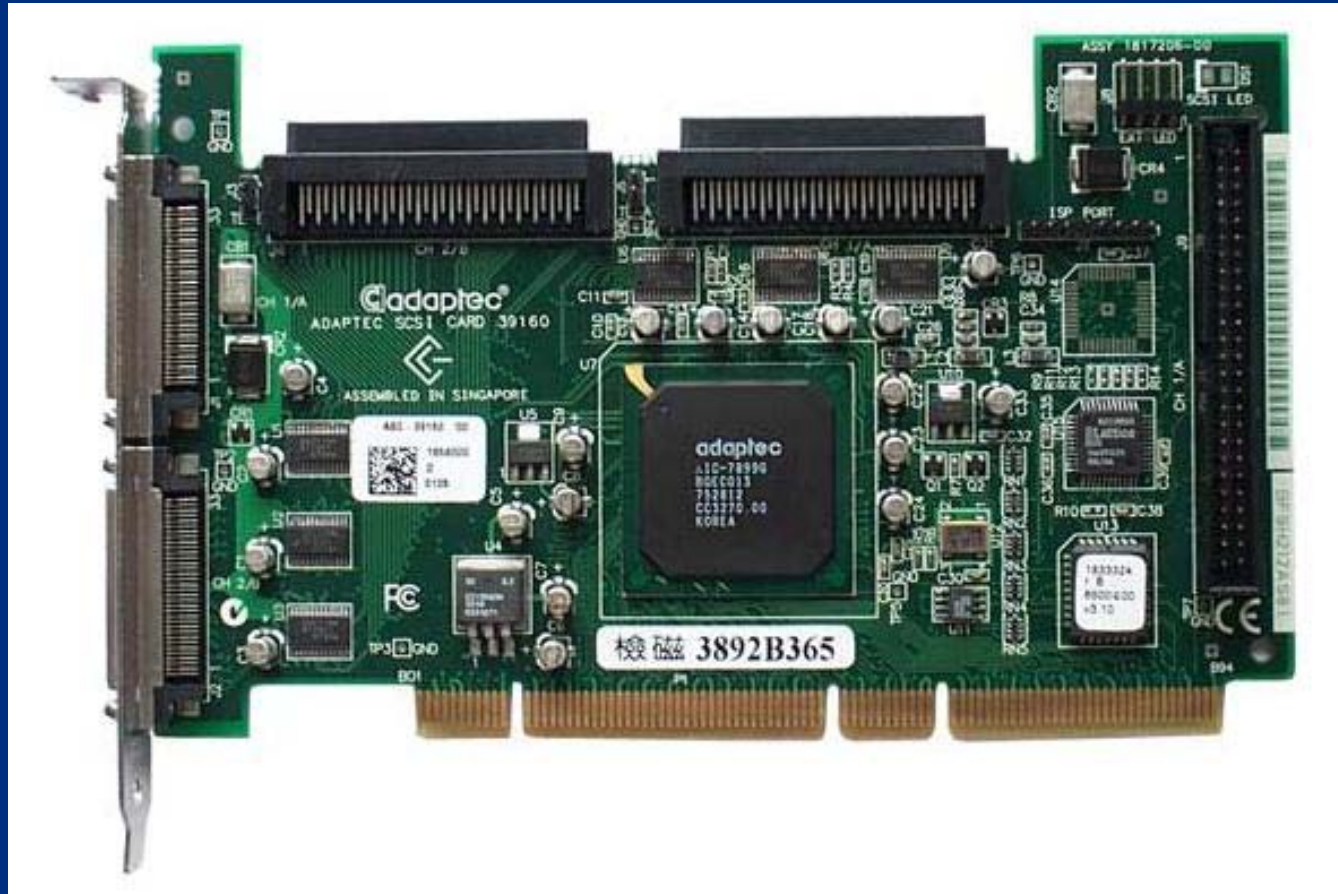
- When one device wants to communicate with system bus, data passes through host adapter
- Because SCSI bus operates like a chain, end of chain must be terminated
- Most computers can support up to four host adapters
- SCSI bus can be either 8-bit or 16-bit
- 16-bit bus is typically named wide SCSI



*U.S. Department of
Homeland Security*

United States
Secret Service

Example of SCSI Card and Cable



U.S. Department of
Homeland Security

United States
Secret Service

Serial Attached SCSI (SAS)

- Serial Attached SCSI (SAS) is another serial bus technology with similarities to both SATA and SCSI
- SAS uses same communication protocols as SCSI to transmit data and same type of connection cables as SATA
- SAS controller is backwards compatible with SATA devices



*U.S. Department of
Homeland Security*

United States
Secret Service

Serial Attached SCSI (SAS)

- A SATA hard drive can be connected to an SAS controller
- Allows less expensive SATA drives to be utilized on SAS systems while providing upgrade path to higher end SAS hard drives
- SATA controllers do not support SAS devices



*U.S. Department of
Homeland Security*

United States
Secret Service

Solid State Drives (SSD)

- Solid State Drive (SSD) is a storage device for notebooks and desktops that uses solid state memory to store data
- No moving parts in a solid state drive
- No moving parts eliminates some seek time and latency and other electro-mechanical delays attributed to conventional hard drives
- Sizes currently range from 32 GB to 256 GB
- Considered too expensive for widespread use



*U.S. Department of
Homeland Security*

United States
Secret Service

Hybrid Hard Drive (HHD)

- Hybrid drives combine solid state and magnetic disk drives
- Solid state component acts as a cache for hard drive and can be up to 1 GB in size
- As data is saved it is temporarily written to SSD cache
- Only when cache is nearly full, or when new data must be read, magnetic portion of drive spins up



*U.S. Department of
Homeland Security*

United States
Secret Service

Hybrid Hard Drive (HHD)

- Improves hard drive performance and reliability, while reducing heat and noise generated by normal hard drives
- Flash memory, or solid state portion of drive, could be used with Windows Vista's ReadyBoost to increase performance on compatible Vista systems
- As of time of this edit, HHDs are only compatible with Windows Vista-based systems



*U.S. Department of
Homeland Security*

United States
Secret Service

Hard Drive Geometry

- Hard drives are divided into tracks, sectors, heads, and cylinders
- Most MB BIOS chips prior to 1997 do not automatically detect geometry information
- Information usually annotated on sticker fixed to drive
- If not, check user reference manuals for manufacturer's Web site for listing of this information by drive type



*U.S. Department of
Homeland Security*

United States
Secret Service

Hard Drive Geometry

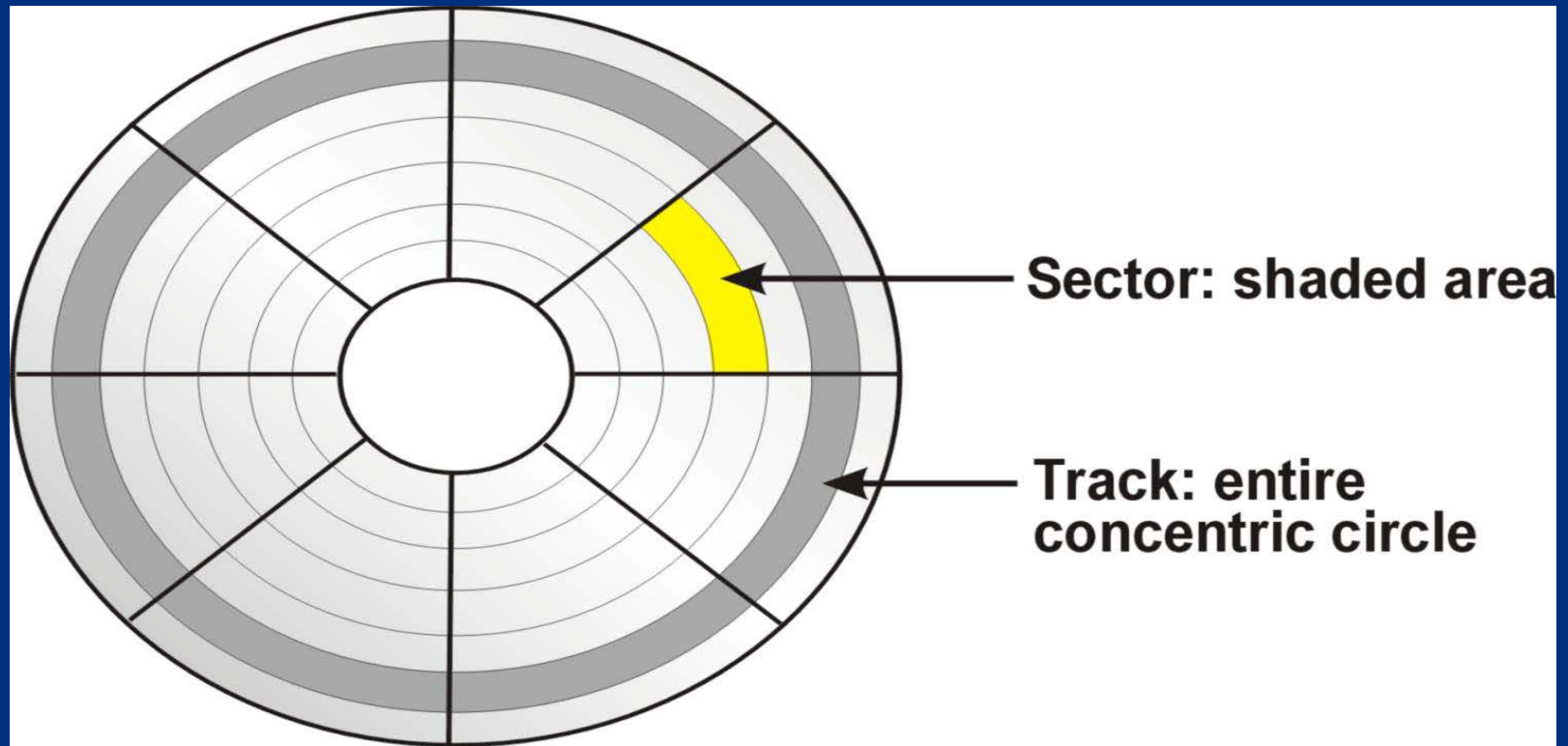
- In computer forensic investigations it is important to know where data is stored on a hard disk
- May be asked during trial about exact location of a file
- May be asked to identify exact location of data by track, sector, and cylinder



*U.S. Department of
Homeland Security*

United States
Secret Service

Hard Drive Geometry



*U.S. Department of
Homeland Security*

United States
Secret Service

Tracks

- Tracks are concentric circular paths placed on both sides of platter
- Specified area that read/write head hovers over
- Arranged starting at center of platter progressing to outer edge
- Measured in density called tracks per inch (TPI)



*U.S. Department of
Homeland Security*

United States
Secret Service

Tracks

- First PC hard disks in 1982 had 200-300 TPI
- Today, drives have over 100,000 TPI
- Tracks uniform on every platter on drive
- A *cylinder* is formed by alignment of the same tracks on all platters



U.S. Department of
Homeland Security

United States
Secret Service

Sectors

- Sectors are shaped segments of tracks
- Each sector holds 512 bytes of data
- With today's technology, each track can have between 17 and 100 or more sectors



*U.S. Department of
Homeland Security*

United States
Secret Service

Heads

- Heads on platter represent specific side of platter
- Sometimes confused with the read/write heads, which are devices that relay data to and from platters



*U.S. Department of
Homeland Security*

United States
Secret Service

Cylinders

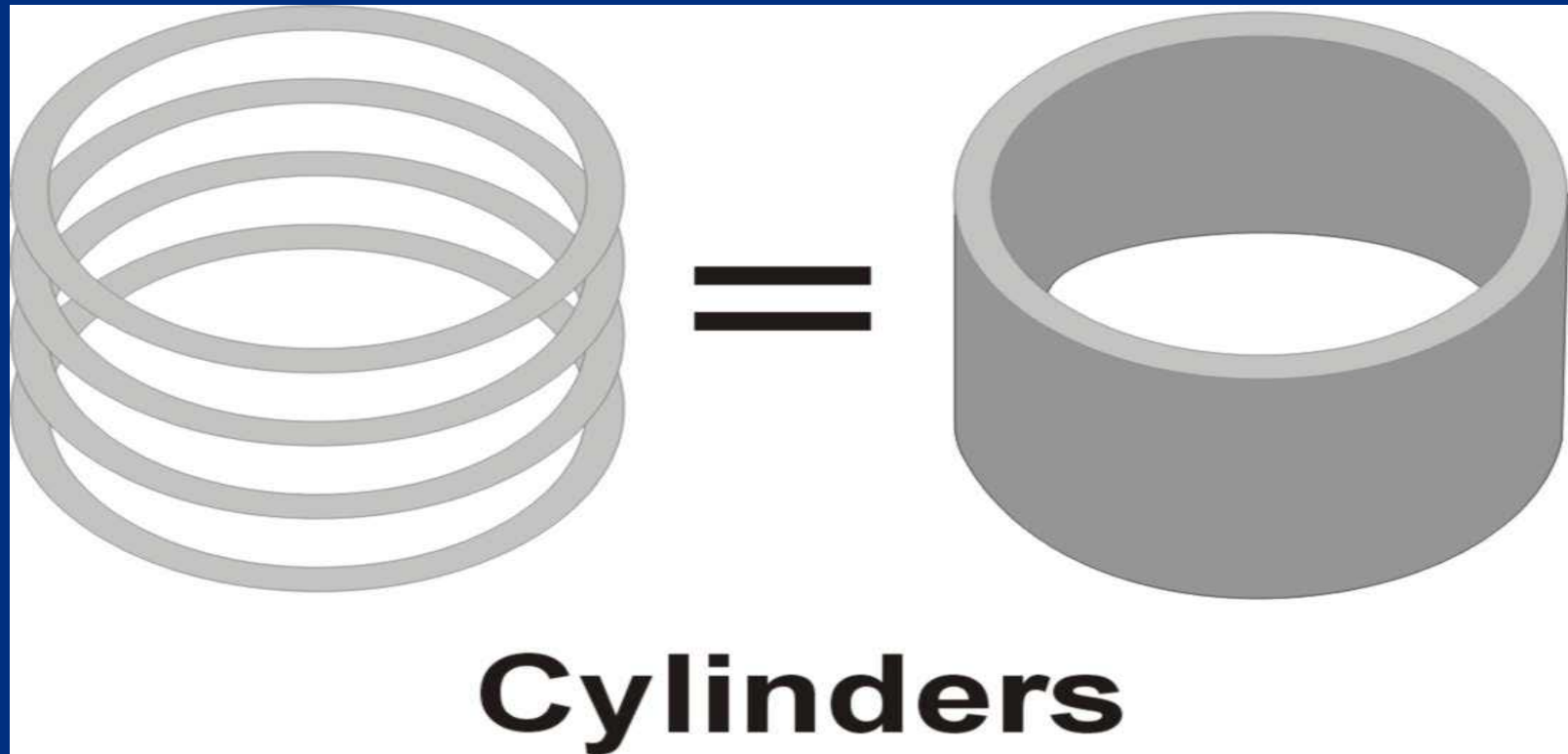
- All platters in a stack are aligned with each other
- Platters move in unison
- A cylinder is formed by identically positioned tracks on every platter



*U.S. Department of
Homeland Security*

United States
Secret Service

Cylinders



*U.S. Department of
Homeland Security*

United States
Secret Service

Clusters

- A group of one or more sectors that form smallest addressable area of storage on disk
- Although the smallest unit of disk space used by an operating system, sizes vary and depend upon OS and partition size of disk



*U.S. Department of
Homeland Security*

United States
Secret Service

RAID

- Redundant Array of Independent Disks (RAID) is a method of combining multiple hard drives and storing data in different locations on those drives at the same time
- Instead of writing data to individual drives, such as drive C and drive D, a RAID allows OS and user to view and use drives C and D as one logical drive
- Using multiple drives that appear as one logical drive instead of using one large hard drive allow for greater performance, capacity, and reliability



*U.S. Department of
Homeland Security*

United States
Secret Service

RAID

- Two methods of writing to RAID:
 - Striping
 - Mirroring
- Various types of RAIDs are produced using different combinations of striping, mirroring, error correction, and parity
- RAIDs are created using software or hardware methods



*U.S. Department of
Homeland Security*

United States
Secret Service

The most common types of RAIDs

- RAID 0
- RAID 1
- RAID 3
- RAID 4
- RAID 5
- RAID 6
- RAID 0+1
- RAID 1+0



*U.S. Department of
Homeland Security*

United States
Secret Service

Striping

- *Striping* involves partitioning each drive's storage space into units ranging from 512 bytes to several megabytes
- Data is written in bytes or groups of bytes across multiple drives as specified by interleave ratio
- More than one drive reads and writes data at same time
- Performance is greatly enhanced



U.S. Department of
Homeland Security

United States
Secret Service

Mirroring

- A technique that stores same data on a pair of disks
- Mirroring ensures an exact duplicate of drive always exists
- Provides full fault tolerance



*U.S. Department of
Homeland Security*

United States
Secret Service

Parity

- A method of checking data when it is copied from one storage place to another to ensure that data has not been lost, overwritten or corrupted
- When a group of bits are copied, an additional parity bit (binary digit) is added
- Parity bit provides ability to ensures that data has been copied successfully



*U.S. Department of
Homeland Security*

United States
Secret Service

Parity

- In RAID, parity is used for data recovery
- It is implemented through *exclusive OR (XOR)*, a logical process that returns a value of “1” if two data bits are not the same
- If any two bits are the same (both 1s or both 0s), result is a 0
- If they are 1 and 0, result is a 1



U.S. Department of
Homeland Security

United States
Secret Service

XOR Process

Data Bit A	Data Bit B	Output
0	0	0
0	1	1
1	0	1
1	1	0



*U.S. Department of
Homeland Security*

United States
Secret Service

XOR Process

- Compares each data bit in data to get XOR result or “parity data”
- Below is an example of how parity data is calculated:
 - Data A = 10100101
 - Data B = 11110000
 - Parity Data = 01010101
- Data A, B, and parity data are on separate drives in RAID
- Corrupt, missing data can be reconstructed using remaining two drives through same XOR process.



*U.S. Department of
Homeland Security*

United States
Secret Service

ECC

- Error Correction Code or Error Checking and Correcting (ECC) looks for errors in data being read or transmitted
- Unlike parity that resends faulty information, ECC attempts to correct information
- ECC uses mathematical code to describe each 64-bit word and sends code with data
- When data is about to be stored, code is regenerated
- If match, data saved, if codes are different, original code used to correct bits



*U.S. Department of
Homeland Security*

United States
Secret Service

RAID 0

- RAID 0 implements striped disk array without mirroring, ECC, or parity
- Data simply placed across several drives allowing each drive to read and write data at same time
- Provides best efficiency and performance, but no fault tolerance



*U.S. Department of
Homeland Security*

United States
Secret Service

RAID 1

- RAID 1, also known as disk mirroring, writes same data to a pair of hard drives
- Cost 100% in overhead
- Provides for best fault tolerance



*U.S. Department of
Homeland Security*

United States
Secret Service

RAID 3

- RAID 3 implements striping small amounts of data across several hard drives
- One drive assigned to store parity information
- Some RAID controller card manufacturers do not support this type of architecture because a RAID 5 with small stripes yields similar results



*U.S. Department of
Homeland Security*

United States
Secret Service

RAID 5

- Implements striping large amounts of data across several hard drives
- Storage of parity bit is rotated throughout all attached drives
- Requires minimum of three drives
- Provides full fault tolerance



*U.S. Department of
Homeland Security*

United States
Secret Service

RAID 0+1

- RAID 0+1 implements a mirrored array of RAID 0 drives
- Minimum of four drives required
- Offers excellent performance and fault tolerance



*U.S. Department of
Homeland Security*

United States
Secret Service

Logical Block Addressing

- Process that assigns linear numbers to all sectors on a drive
- Process extends drive's storage capacity from normal 528MB
- Older MBs' BIOS types or operating systems may require LBA to be translated into CHS geometry
- Translation performed automatically if required
- 28-bit LBA supports a partition as large as 137GB
- 48-bit LBA theoretically supports a single drive with storage of 144 petabytes



*U.S. Department of
Homeland Security*

United States
Secret Service

Zoned Bit Recording

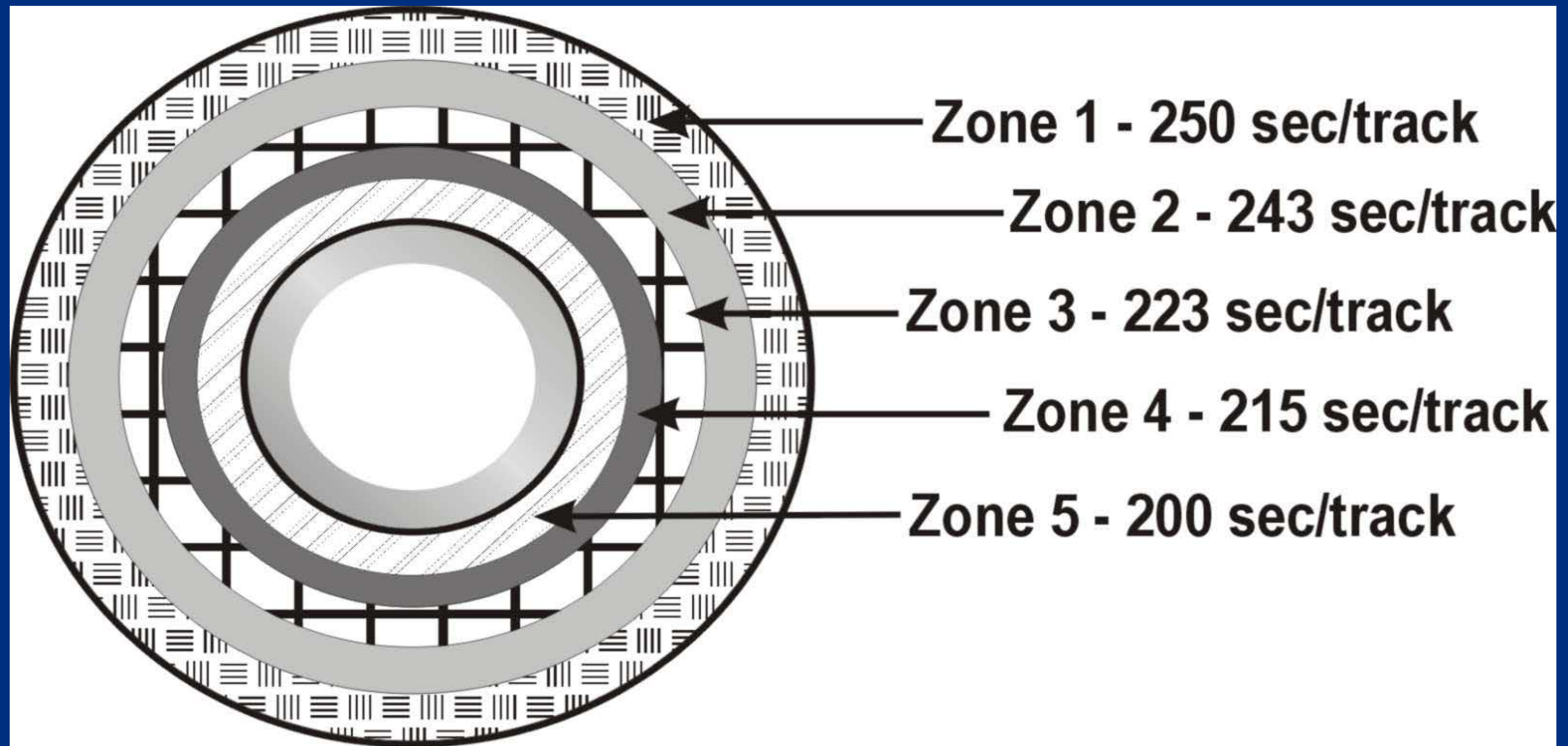
- Reassigns sectors on disk according to physical size of track
- Lessens wasted storage space on outer sections of hard drive
- Data on small tracks near center of disk, written closer together than data on larger outer tracks
- Outermost tracks can contain more sectors per track than smaller inner tracks
- Drive controller can recognize the variable number of sectors per track in different zones
- Set during low-level format



*U.S. Department of
Homeland Security*

United States
Secret Service

Hard Drive with Zoned Bit Recording



*U.S. Department of
Homeland Security*

United States
Secret Service

Perpendicular Recording

- Perpendicular recording technology increases amount of storage space on hard drive
- Using perpendicular recording, manufacturers have produced micro-drives with over 100GB of storage on a 1.8" drive, a 320GB 2.5" laptop drive, and a 3.5" drive with over 1 terabyte of storage
- Can increase storage density of a hard drive by almost ten times compared to longitudinal recording



*U.S. Department of
Homeland Security*

United States
Secret Service

Perpendicular Recording

- Perpendicular recording vertically records bits of a sector to a hard drive
- Stacking bits vertically increases amount of storage density
- Allows more data to be stored with less risk of corruption



*U.S. Department of
Homeland Security*

United States
Secret Service

Hard Drive Formatting

- A hard drive must be prepared before using it to store data
- Preparation process involves two *formatting* steps (low-level formatting and high-level formatting) with a *partitioning* step between them



U.S. Department of
Homeland Security

United States
Secret Service

Low-level Formatting

- Purpose of low-leveling formatting, also called physical formatting, is to set drive geometry by first setting tracks and then dividing them into sectors



*U.S. Department of
Homeland Security*

United States
Secret Service

Partitioning

- To use a hard drive, it must be partitioned
- On most newly purchased computers the original equipment manufacturer (OEM) has partitioned drive as single partition
- Partition designated as C: drive on system
- Partitioning drive into multiple drives offers many benefits



*U.S. Department of
Homeland Security*

United States
Secret Service

Partitioning

- Many ways to partition a drive
- Operating systems provide the tools
- MS-DOS uses FDISK utility
- Windows XP uses Disk Management
- Some distributions of Linux use Disk Druid
- Interfaces look different but results are the same



*U.S. Department of
Homeland Security*

United States
Secret Service

Partitioning

- Only two types of partitions: Primary and Extended
- At least one primary partition required to boot computer from hard drive
- Extended partitions typically used for storing data and applications
- Extended partitions cannot be used to boot computer



*U.S. Department of
Homeland Security*

United States
Secret Service

Partitioning

- Hard drives can support up to four primary partitions or three primary partitions and one extended
- The FDISK utility only recognizes one primary partition per physical drive so DOS and Windows 9x/ME can only have one primary partition per drive
- Linux, Unix, Windows 2000, XP and Vista can all support four primary partitions



*U.S. Department of
Homeland Security*

United States
Secret Service

Partitioning

- Once primary partition is created, drive is ready for high-level formatting
- Extended partitions require one additional step before format
- It must be further organized into logical drives which can be accomplished with the same partitioning utilities mentioned previously
- Once partitions and logical drives are created high-level formatting may be done



*U.S. Department of
Homeland Security*

United States
Secret Service

High-level Formatting

- High-level formatting, also called *logical formatting*, is performed by operating system
- High-level formatting writes operating system-dependent file structures to drive so it can manage and store data
- Establishes boot record, file allocation table, and root directory
- Process also scans disk for areas that are unable to store data and marks and isolates them as bad sectors



U.S. Department of
Homeland Security

United States
Secret Service

MS-DOS FAT

- MS-DOS, Windows 9x, and Windows ME make use of MS-DOS-based FDISK utility
- FDISK responsible for creation and deletion of partitions and logical drives
- Partitions cannot be altered easily once created
- File Allocation Table (FAT) partitions cannot be resized without use of third-party software
- Original partitions must be deleted and new partitions created



*U.S. Department of
Homeland Security*

United States
Secret Service

FAT File System Characteristics

- Each partition or logical drive contains a FAT
- FAT manages a list of where files begin and end on drive
- List is constantly updated with new information as files are saved, deleted, renamed or moved



*U.S. Department of
Homeland Security*

United States
Secret Service

FAT File System Characteristics

- Critical that list stay up to date and intact to allow operating system to access files
- So critical that latest backup copy of the FAT is saved in another area on hard drive
- Backup copy used to restore original if damaged or altered



*U.S. Department of
Homeland Security*

United States
Secret Service

FAT File System Characteristics

- FAT16 used a 16-bit length number to identify various clusters on a hard drive
- Limited addressable capacity of a hard drive to 65,526 clusters, or 2GB of data
- Using FAT16 on drives larger than 2GB requires partitioning drive to fully use drive's capacity



*U.S. Department of
Homeland Security*

United States
Secret Service

FAT File System Characteristics

- FAT32 uses a 32-bit length number to identify all clusters on a hard drive
- Increase allows file system to address approximately 268,400,000 clusters, or approximately 2 terabytes of information



*U.S. Department of
Homeland Security*

United States
Secret Service

FAT Drive Identification

- FAT 16/32 systems can support up to two partition types per hard drive
- Types are primary and extended
- Extended partition contains logical drives
- Each primary partition and each logical drive within extended partition, assigned a drive letter starting with C
- When assigning drive letters, primary partitions take precedence over logical drives



*U.S. Department of
Homeland Security*

United States
Secret Service

NTFS

- Windows 2000 and Windows XP can operate in a FAT32 or FAT16 environment, but default file system is NTFS
- NTFS required to install Windows Vista Operating System
- NTFS is more stable than FAT system and offers such benefits as file compression and data encryption
- NTFS supports *dynamic volumes* which allow partitions to be added or extended without loss of data



U.S. Department of
Homeland Security

United States
Secret Service

NTFS Partitioning and Formatting

- Partitioning is not performed at command prompt level
- FDISK neither supports nor offers NTFS as partitioning option
- Partitioning of primary partition occurs during installation
- If additional hard drives are added to system, partition and format using an integrated tool



*U.S. Department of
Homeland Security*

United States
Secret Service

NTFS Partitioning and Formatting

- Windows Disk Management tool allows addition, deletion or modification of partitions
- Can be used to display general volume information including file system type, amount of available space and total capacity
- Can also be used to convert partition from FAT16/32 to NTFS



*U.S. Department of
Homeland Security*

United States
Secret Service

NTFS Partitioning and Formatting

- Number of ways that a partition can be formatted or reformatted to NTFS
- Disk Administrator can be used to format
- Partition can be formatted via right clicking on My Computer and selecting appropriate options
- Format command can also be executed via command line



*U.S. Department of
Homeland Security*

United States
Secret Service

NTFS File System Characteristics

- NTFS utilizes MFT (Master File Table) to track files and locations on volume
- MFT is similar to FAT in that it maps location of directories and folders and is updated whenever a file is accessed, changed, deleted or added to volume
- Significant differences between a MFT and FAT



*U.S. Department of
Homeland Security*

United States
Secret Service

NTFS File System Characteristics

- FAT can be thought of as a static fixed-sized chart that cannot change in size
- The MFT is dynamic, relational database that can grow in size if necessary
- The MFT is created when drive (or volume) is formatted for NTFS specifications with certain amount of contiguous space reserved for MFT expansion



*U.S. Department of
Homeland Security*

United States
Secret Service

NTFS File System Characteristics

- Expansion area sometimes called “MFT Zone”
- Initially, zone is approximately 12 percent of total volume capacity but can grow if needed
- Most NTFS volumes are no larger than 2 terabytes in size
- Dynamic nature of MFT allows NTFS volume to reach 16 exabytes, equivalent to approximately 16,000,000 terabytes in capacity!



*U.S. Department of
Homeland Security*

United States
Secret Service

NTFS Drive Identification

- Assigning drive letters in NTFS somewhat different than in FAT
- Drive letters are assigned as they are discovered by operating system
- Drive letters do not change when devices are added or removed from system



*U.S. Department of
Homeland Security*

United States
Secret Service

Linux

- Linux offers opportunity to partition hard drive during installation of operating system
- Fedora, a Linux distribution based off former Red Hat Linux, uses Disk Druid utility
- Disk Druid offers graphical, mouse driven menu system that creates partitions based on installer's preferences



*U.S. Department of
Homeland Security*

United States
Secret Service

Linux

- Linux offers an FDISK program similar to DOS-based utility
- Can be used to create and remove various partitions as well as view status of a hard drive's configuration
- Linux partition can be formatted to a number of file systems, including:
 - Second Extended File System (ext2)
 - Third Extended File System (ext3)
 - Reiser File System



*U.S. Department of
Homeland Security*

United States
Secret Service

File System Characteristics ext2

- Ext2 introduced in 1993 and became standard file systems for many different versions of Linux
- File system could be modified to fit needs of end user
- Offers more features than earlier Linux file systems including better space allocation, larger partition sizes (up to 16 terabytes in size), and long file names support
- Most notable, ext2 was configurable



*U.S. Department of
Homeland Security*

United States
Secret Service

File System Characteristics ext3

- Default file system in most Linux distributions Since 2001
- In comparison to ext2, ext3 provides greater reliability by taking advantage of journaling, which offers a more reliable file recovery process than ext2
- Journaling tracks all items related to main data areas of disk
- Journaling can recreate anything lost or corrupted due to a problem or failure



*U.S. Department of
Homeland Security*

United States
Secret Service

File System Characteristics ext3

- Ext3 systems do not require file system check after unclean shutdown
- System checks occur only in extreme circumstances such as hardware failures
- Recovering from a power failure takes much less time when using ext3 file system as opposed to ext2



*U.S. Department of
Homeland Security*

United States
Secret Service

File System Characteristics ext3

- Ext3 also boasts a faster read/write speed than ext2
- Ext3 uses journal to not only protect files, but also to optimize hard drive's read-write head motions
- Read/write process is completed in a more efficient manner



*U.S. Department of
Homeland Security*

United States
Secret Service

File System Characteristics ext3

- Volumes using ext2 file system can easily be converted to ext3 standard with one command using tune2fs program
- Partitions do not have to be removed and recreated
- Journal system is updated to ext3 format without loss of data
- Ext3 file system can manage partitions up to 16 terabytes in size



*U.S. Department of
Homeland Security*

United States
Secret Service

Reiser

- Some similarities with extended file systems
- Can address a partition up to 16 terabytes in size
- Reiser is considered a more robust file system
- Like ext3, Reiser takes advantage of journaling for greater file reliability
- Reiser provides capability of online resizing allowing file system to automatically extend size of partition as needed



*U.S. Department of
Homeland Security*

United States
Secret Service

Reiser

- Only allows for extending partition not shrinking
- Tools are available to accomplish both growing and shrinking of file system while offline
- Development of Reiser version 3 has been stopped
- Focus of development has shifted to version 4



*U.S. Department of
Homeland Security*

United States
Secret Service

File System Characteristics ext4

- Ext4 still currently under development, primary improvements include
 - Support for volume sizes of up to 1 exbibyte
 - Support for large file size up to 2 Terabyte
 - Ability to undelete files
 - Extents - a continuous area of storage reserved for a file
 - Persistent file pre-allocation
 - Online defragmentation



*U.S. Department of
Homeland Security*

United States
Secret Service

Linux Drive Identification

- Drive identification process in Linux differs from those used in FAT or NTFS
- Identification values are assigned based on how device is connected to MB, jumper settings, and relationship to other storage devices



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 2 – Floppy Drives and Removable Media

- Floppy Disk Drives
- Removable Media



*U.S. Department of
Homeland Security*

United States
Secret Service

Floppy Disk Drives

- Floppy disks are storage devices used to move information from one system to another and to make file backups
- There are two different types of floppy disks available, 5.25-inch Disk and 3.5-inch



*U.S. Department of
Homeland Security*

United States
Secret Service

Floppy Disk Drives 5.25-inch



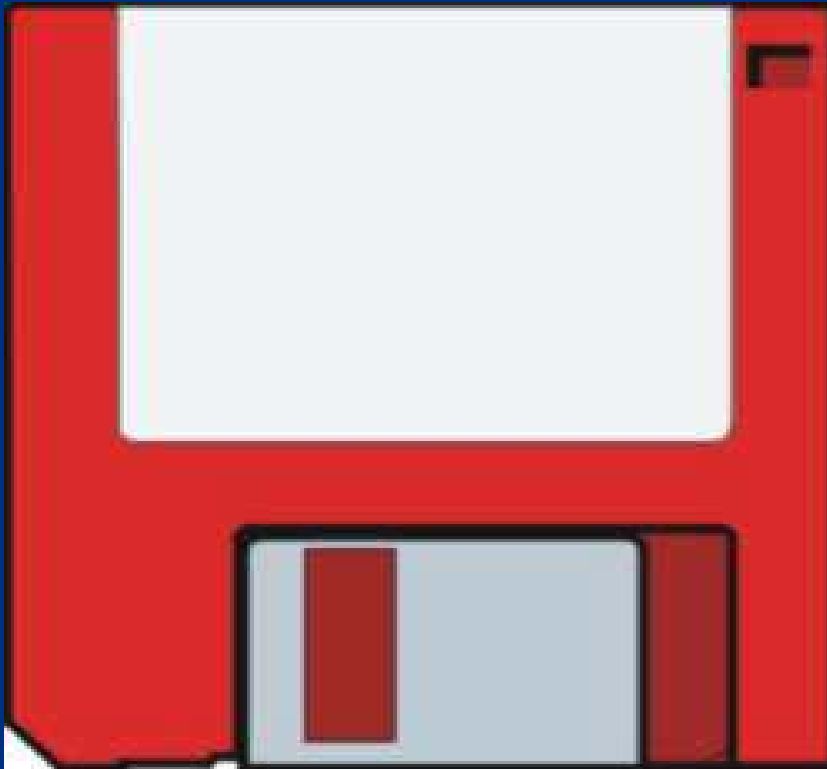
- Double-sided, high-density disk.
- 80 tracks with 15 sectors per track
- 4 KB clusters, and either 420 KB or 1.2 MB of storage
- Nearly obsolete, may be found in systems dated before 1994



*U.S. Department of
Homeland Security*

United States
Secret Service

Floppy Disk Drives 3.5-inch



- Most PCs today use 1.44 MB 3.5 inch disks for data transfer and backup
- Integration in newer computers becoming rare
- Disks are encased in hard plastic shell and come in three density types



*U.S. Department of
Homeland Security*

United States
Secret Service

Floppy Disk Drives 5.25-inch

- Double Sided/Extra High Density: 80 tracks; two sides, 36 sectors per track, 4 KB clusters; 2.88 MB of storage space
- Double Sided/High Density: 80 tracks; 2 sides, 18 sectors per track, 4 KB clusters; 1.44 MB of storage space
- Double Sided/Double Density: 80 tracks; 2 sides, 9 sectors per track, 4 KB clusters; 720 KB of storage space



*U.S. Department of
Homeland Security*

United States
Secret Service

Floppy Drive Controllers

- Most floppy drive controllers are now found on super I/O chip
- In past, floppy disk controller was found on a separate ISA slot card



*U.S. Department of
Homeland Security*

United States
Secret Service

Characteristics of Floppy Drive Controllers

- Connected to MB for data input/output via a 34-pin ribbon cable that has a twisted segment to differentiate drive A from drive B
- Unlike controller connections for a hard drive, floppy controller has no standard location for pin 1
- Some drives locate pin 1 close to power connector while others place it away from power connector
- Modern transfer rate has been standardized to approximately 1 Mb/sec



*U.S. Department of
Homeland Security*

United States
Secret Service

Removable Media

- Floppy drives almost completely replaced by other forms of removable media
- Demand for storage of large amounts of data
- Trend began with devices such as ZIP drives and LS 120 drives, continues now with flash drives
- Removable media can be divided into several categories: magnetic media, magneto-optical media, DVDs, CD-ROMs, USB flash drives, and external drives



*U.S. Department of
Homeland Security*

United States
Secret Service

SyQuest Magnetic Media Drives

- Uses 5.25 inch and 3.5 inch disk cartridges that use a rigid platter housed in a plastic cartridge
- Disk capacity: 5.25 inch disk holds 44 MB and 88 MB and 3.5 inch disk holds 105 MB and 270 MB
- Used with ATAPI and SCSI interface models
- Drives not widely used but may be found in older computer systems



*U.S. Department of
Homeland Security*

United States
Secret Service

Iomega ZIP Magnetic Media Drives

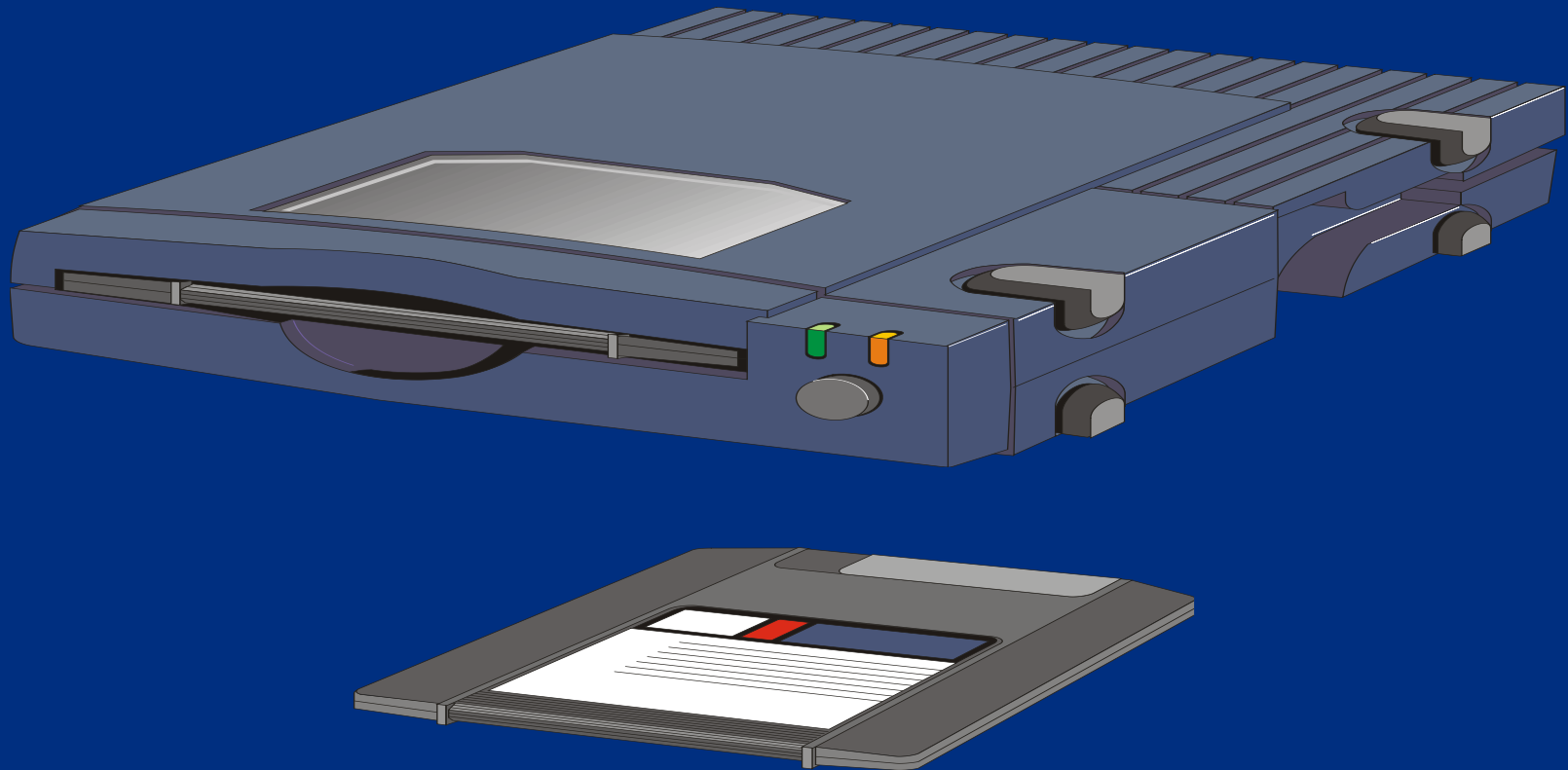
- Uses a proprietary disk format, which is a 3.5 inch disk cartridge with a flexible platter housed inside a plastic cartridge
- Disks are about twice as thick as 3.5 inch floppy
- Disk capacity is 100 MB, 250 MB, and 750 MB
- External models use SCSI, parallel, and USB interfaces and internal models use SCSI or ATAPI interfaces



*U.S. Department of
Homeland Security*

United States
Secret Service

Iomega ZIP Drive and Cartridge



*U.S. Department of
Homeland Security*

United States
Secret Service

Magneto-optical Drives

- *Magneto-optical drives* provide magnetic, high density storage
- Data written to drives by a precise laser beam that heats a tiny spot in disk's alloy to Curie point of 300 degrees
- Allows molecules to be realigned when subjected to magnetic field located on opposite side of disk



U.S. Department of
Homeland Security

United States
Secret Service

Magneto-optical Drives

- To read stored data on drive, weaker laser beam is used to focus on tracks
- Crystals in alloy polarize the light from the laser
- Reflective beam is read by a photodiode that translates reflective light to ones and zeros
- Data then passed on



*U.S. Department of
Homeland Security*

United States
Secret Service

Super Floppy or Floptical Drive

- The LS-120 drive, known as the *super floppy or floptical*, can store twenty times more data than a conventional floppy
- Most super floppies hold 120 MB of data on a 3.5-inch disk
- Sony has a 200 MB model
- Nearly identical in appearance to standard floppy disks and can read/write to floppy disks
- Developed by 3M, O.R. Technologies, and Mastushita-Kotobuki Industries



U.S. Department of
Homeland Security

United States
Secret Service

Super Floppy or Floptical Drive

- Uses same ferrite materials common to floppy drives
- Use a special optical mechanism to align magnetic read/write heads over data tracks
- Servo track information that laser uses to guide read/write heads is etched into disk by manufacturer
- If formatted in a standard floppy drive, storage capacity will be reduced to 1.44 MB
- Drives may be found in ATAPI and SCSI systems



*U.S. Department of
Homeland Security*

United States
Secret Service

Tape Drives

- Tape drives used primarily to backup entire systems
- Tape drives come with proprietary software and newer models have ATAPI and SCSI interfaces
- The two types of tape storage include magnetic tapes and digital audio tape (DAT)



*U.S. Department of
Homeland Security*

United States
Secret Service

Magnetic Tape Storage



- Operate much like old reel-to-reel recording systems
- Two sizes: 1) data cartridge (6 inches by 4 inches by 0.675 inch) 2) mini cartridges (3.2 inches by 2.4 inches by 0.4 inch)
- Stores from 2GB to over 500GB of data



*U.S. Department of
Homeland Security*

United States
Secret Service

DAT Storage

- Records in a digital format using magnetic technology
- Tape size is a little smaller than a cassette tape
- Available in two primary formats: 1) 4mm cartridge that stores up to 36GB of uncompressed data and 2) 8mm cartridge that stores up to 80GB of uncompressed data
- A third format, Digital Linear Tape (DLT), stores between 35GB and 800GB of data and is only used with high-end data servers



*U.S. Department of
Homeland Security*

United States
Secret Service

Compact Disc Read Only Memory (CD-ROM)

- CD-ROM is a disc format used to hold text, graphics and hi-fi stereo sound
- Very similar to an audio CD, but uses a different format for recording data
- An audio CD player cannot play CD-ROMs, but CD-ROM players can play audio discs



*U.S. Department of
Homeland Security*

United States
Secret Service

How Data is Stored on CD-ROM

- Information is stamped into disc as a series of pits and lands when manufactured
- Pits are small raised areas in tracks on CD-ROM separated by flat spaces (lands)
- Back of a CD-ROM is a highly reflective surface



*U.S. Department of
Homeland Security*

United States
Secret Service

How Data is Stored on CD-ROM

- When laser beam shines up through the disc, light is reflected back
- When light hits edge of a pit, light is not reflected back
- When light hits a land, it is reflected back
- Microprocessors in drive translate light and dark transitions as 1s and 0s



*U.S. Department of
Homeland Security*

United States
Secret Service

Compact Disc Recordable (CD-R)

- CD-R is a form of CD-ROM technology that writes to a disc
- Each disc can be written to only once
- A CD-R drive cannot stamp pits into disc
- Instead, uses a layer of dye to simulate pits and lands



*U.S. Department of
Homeland Security*

United States
Secret Service

Compact Disc Recordable (CD-R)

- To record, laser burns dye to simulate pits and does not burn areas for lands
- To read, laser beam is reflected back from non-burnt areas (lands) and is not reflected back from burnt areas (pits)
- Drive interprets both



*U.S. Department of
Homeland Security*

United States
Secret Service

Compact Disc Re-writable (CD-RW)

- CD-RW can record, erase, and re-record data on same disc up to 1,000 times
- Instead of stamped pits or dye, CD-RWs use a phase change technology that involves a crystalline layer
- Process uses high intensity laser pulse that turns crystalline natural state (reflective) to an amorphous one (dull)



*U.S. Department of
Homeland Security*

United States
Secret Service

Compact Disc Re-writable (CD-RW)

- When disc is read, it uses this dull/reflective state to simulate pits and lands
- To erase and re-record data, CD-RW uses a medium intensity pulse to restore crystalline surface to a reflective state



*U.S. Department of
Homeland Security*

United States
Secret Service

DVD

- DVD is commonly termed Digital Video Disc as means to describe technology
- DVD is far more capable than just storing and playing digital video
- DVD is a group of disk formats that store data, video, or audio information with capacities between 4.7GB and 8.54GB
- Generally disk is 120mm in diameter and 1.2mm thick



*U.S. Department of
Homeland Security*

United States
Secret Service

DVD

- Reflective surfaces embedded in polycarbonate resin hold data as pits and lands in tracks much smaller and closer together than those on CD
- All DVD drives feature backward compatibility to read CD media



*U.S. Department of
Homeland Security*

United States
Secret Service

DVD-ROM

- Data, be it audio, video, or software, is molded into disk when manufactured
- Unlike CD media, DVD media has its reflective data layer more deeply protected in structure of disk



*U.S. Department of
Homeland Security*

United States
Secret Service

User-Recordable DVD

- Data is written or “burned” into a disk by user with a write capable drive
- Currently, there are six different formats of writable DVD
- Compatible media must be used in appropriate drive to make a recording
- Once written, all DVD disk types (except DVD-RAM) can be read in other DVD drive types



*U.S. Department of
Homeland Security*

United States
Secret Service

Recordable DVD Media Types

DVD-RAM	Once formatted, disk together with its drive can be treated as if it were a hard disk drive. Re-writable up to 100,000 times.
DVD-R	Write-once, read many times
DVD-RW	Re-writable up to 1,000 times
DVD+R	Write-once, read many times
DVD+RW	Re-writable up to 1,000 times
DVD+R DL	Dual layer write once, read many times



*U.S. Department of
Homeland Security*

United States
Secret Service

DVD Capacity Comparison

Format	Capacity	Type
Single Sided, Single Layer	4.7 billion bytes	“DVD-5”
Single Sided, Dual Layer	8.5 billion bytes	“DVD-9”
Double Sided, Single Layer	9.4 billion bytes	“DVD-10”
Double Sided, Dual Layer	17 billion bytes	“DVD-18”



*U.S. Department of
Homeland Security*

United States
Secret Service

HD-DVD and Blu-ray

- Introduced in 2006, HD-DVD and Blu-ray are two rival High Density DVD formats
- Each format backed by competing groups of equipment manufacturers
- HD-DVD has data capacity of 15GB for single-layer disks and 30GB for dual-layer disks



*U.S. Department of
Homeland Security*

United States
Secret Service

HD-DVD and Blu-ray

- In late 2007 a new format was approved, allowing for three layers to store a capacity of 51GB
- Blu-ray disks can hold 25GB for single layer disks and 50GB for dual-layer disks
- Laboratory tests have successfully tried up to eight layers for a total of 200GB per disk



*U.S. Department of
Homeland Security*

United States
Secret Service

USB Flash Drives

- Flash drives allow transport of files between devices
- Offer a very compact, non-volatile storage option for data
- Transfer rate of data is dependent on type and speed of interface used for device
- Small, easily transported, and rewritable
- Uses USB 1.0, 1.1, or 2.0
- Store up to 64GB



*U.S. Department of
Homeland Security*

United States
Secret Service

Memory Cards

- Memory cards are flash memory storage devices common in many electronic devices
- Some devices that may support memory cards are digital cameras, cell phones, portable audio devices, game consoles, mobile computers, etc.
- Large storage capacities and small footprints make this storage technology an excellent companion to many portable electronic devices



*U.S. Department of
Homeland Security*

United States
Secret Service

Compact Flash

- Introduced by Sandisk in 1994
- With storage capacities up to 64GB, commonly found in digital cameras or mini hard drives
- Available in two variations: Type I and Type II



*U.S. Department of
Homeland Security*

United States
Secret Service

Secure Digital (SD)

- Developed by Sandisk, Matsushita, and Toshiba
- Secure Digital format supports up to 16GB of storage and up to 32GB with high-capacity SDHC cards



*U.S. Department of
Homeland Security*

United States
Secret Service

MiniSD

- Provides storage capacities up to 4GB
- These devices can be used in a typical SD slot with use of an adapter



*U.S. Department of
Homeland Security*

United States
Secret Service

MicroSD

- Cards are about size of a penny and provide storage capacities up to 8GB
- Can be used in the larger SD and MiniSD slots with use of an adapter
- A high capacity implementation, MicroSDHC, allows for capacities up to 8GB



*U.S. Department of
Homeland Security*

United States
Secret Service

Memory Stick

- This memory is developed by Sony
- Term “Memory Stick” can refer to whole memory stick lineup of products
- Include Memory Stick Pro, Memory Stick Duo/Pro Duo, Memory Stick Micro, and Memory Stick Pro-HG



*U.S. Department of
Homeland Security*

United States
Secret Service

External Drives

- External drives are available in USB, FireWire, and eSATA
- Hot swappable and easily transported from one system to another
- USB and FireWire connections are recognized by operating systems such as Windows XP and many versions of Linux



*U.S. Department of
Homeland Security*

United States
Secret Service

External Drives

- The eSATA has a special adapter and cable, which eliminates protocol issues of converting drive's native signal to the serial port adapter
- Allows higher transfer rates
- Restricts portability of drive to computers equipped for eSATA



*U.S. Department of
Homeland Security*

United States
Secret Service



*U.S. Department of
Homeland Security*

United States
Secret Service

Module 3 – Input/Output Components



*U.S. Department of
Homeland Security*

United States
Secret Service

You will learn ...

- Input/Output Devices and Ports
- BIOS and System Initialization



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 1 – Input/Output Devices and Ports

- Input/Output Overview
- Input Devices
- Output Devices
- Input/Output Ports
- Modems
- PC Cards



*U.S. Department of
Homeland Security*

United States
Secret Service

Input/Output Overview

- Most hardware components found on a PC can be categorized as either an input or output device.
- Modems are the exception because they transmit and receive information



*U.S. Department of
Homeland Security*

United States
Secret Service

Input Devices

- Keyboard
- Mouse and other pointing devices
- Game controllers
- Scanners



*U.S. Department of
Homeland Security*

United States
Secret Service

Output Devices

- Monitors
- Video Adapter Cards
- Printers



*U.S. Department of
Homeland Security*

United States
Secret Service

Input Devices - Keyboard Devices

- Keyboard is the primary input component for a computer
- Many new features added to keyboard in recent years, such as additional short cut keys
- Basic way a keyboard works has remained the same since first IBM PC in early 1980s
- Many styles of keyboards with various built-in functions including pointing devices such as trackballs and special keys programmed to launch programs or Web sites



*U.S. Department of
Homeland Security*

United States
Secret Service

How Keyboards Work

- Uses grid of embedded circuits called key matrix
- When key is pressed, change in current, in circuit associated with key, is picked up by keyboard's microprocessor
- Microprocessor generates scan code that is read by computer's BIOS
- BIOS translates scan code into ASCII code which is recognized by application software such as word processing software



*U.S. Department of
Homeland Security*

United States
Secret Service

Input Devices - Pointing Devices

- Come in many shapes and sizes
- Used to control computer by pointing to images instead of using keyboard to type commands
- Mouse, first device developed by Xerox in early 1980s and remains standard
- Other current devices include touchpad, trackball, trackpoint, and game controller



*U.S. Department of
Homeland Security*

United States
Secret Service

Input Devices - Mouse

- Standard pointing device used to navigate system's graphical user interface (GUI)
- Internal electronics sends signals through attached cable to computer's operating system
- Operating system translates signal to move onscreen cursor



*U.S. Department of
Homeland Security*

United States
Secret Service

Input Devices - Touchpad

- Fixed pointing device that uses movement of a finger on touch-sensitive pad to control location of cursor in GUI
- Replaces standard mouse in laptop and notebook computers where space is limited
- Also known as glidepoint



*U.S. Department of
Homeland Security*

United States
Secret Service

Input Devices - Trackball

- Basically an inverted mouse with the ball located on outside of housing
- Contains same connectors as found in standard mouse



*U.S. Department of
Homeland Security*

United States
Secret Service

Input Devices - Trackpoint

- Also called a pointing stick, a small rubber component embedded on the keyboard between G and H keys on a laptop computer
- Move stick to move cursor



*U.S. Department of
Homeland Security*

United States
Secret Service

Input Devices - Gyroscopic Mice

- Gyroscopic mice feature gyroscopes to detect movement while mouse is moved in mid-air
- Such mice normally shaped similar to remote controls and allow for wireless control of a computer from long distances
- Commonly used for conference room and home theater computers



*U.S. Department of
Homeland Security*

United States
Secret Service

Input Devices - Game Controllers

- Also called joysticks, available in wide variety of designs such as steering wheels, flight simulator controls, and pressure pads
- All are input devices for game software
- Joystick has upright stick that controls movement by providing the X-Y axis coordinates of the stick



*U.S. Department of
Homeland Security*

United States
Secret Service

Input Devices - Game Controllers

- Joysticks available in digital or analog compatible formats
- Connect through game ports or USB port
- More expensive controllers can be programmable with macros to allow specific series of actions or commands to be transmitted with single button



*U.S. Department of
Homeland Security*

United States
Secret Service

Input Devices - Scanner

- Used to translate text or pictures into a digitized form computer can read and store
- Scans are delivered to computer as a digital image
- Scanned pictures are code that can be used by graphics software program
- Printed type can be converted into editable text when scanned using optical character recognition (OCR) software



*U.S. Department of
Homeland Security*

United States
Secret Service

Input Devices - Hand-held scanners

- Offer low resolution, 200-400 dots-per-inch (DPI), with 8-bit imaging.
- Scan window only five to seven inches wide
- Wide images require image re-sectioning



*U.S. Department of
Homeland Security*

United States
Secret Service

Input Devices - Flatbed scanners

- Provide photo quality resolution
- Typed sheets and pictures placed facedown on large scan window
- Advantages include high resolution and ability to scan thick documents such as books
- Usually come with their own proprietary image processing software



*U.S. Department of
Homeland Security*

United States
Secret Service

Input Devices - Sheet-fed scanners

- Scan one standard-size sheet at a time
- Resolution can be the same as flatbed scanners



*U.S. Department of
Homeland Security*

United States
Secret Service

Output Devices - Monitors

- Main video display components of PC, include monitor and video adapter, also known as a video card
- Monitor refers to display screen



*U.S. Department of
Homeland Security*

United States
Secret Service

Monitor Classification Criteria

- Diagonal screen size measured in inches
- Desktop PC monitors range in size from 14 to over 40 inches and LCDs in laptops generally range from 6 to 21 inches
- Monitors usually evaluated on two factors, size and resolution
- Display resolution measured in pixels
- Refresh rate ranging from 60Hz to 100Hz



*U.S. Department of
Homeland Security*

United States
Secret Service

Monitor Technologies

- Cathode ray tube (CRT) monitor: Most common type of monitor for desktop systems until the early 2000s
- Liquid crystal display (LCD) monitor: Used in laptops as well as high-end desktop monitors
- Organic Light Emitting Diode (OLED) monitor: Used in laptops as well as desktop monitors



*U.S. Department of
Homeland Security*

United States
Secret Service

Benefits of CRT Monitors

- Sales of CRT monitors have decreased in recent years, though have a few major advantages over LCD monitors
- Color display on CRT monitors is better than LCD, provide a greater color range and depth, beneficial to graphic artists
- LCDs suffer from blurring during fast motion and slower response times in redrawing the screen
- Issues make high-performance CRT monitors beneficial to avid gamers



*U.S. Department of
Homeland Security*

United States
Secret Service

CRT Monitor Resolution

- Resolution of a monitor is measured by pixel density
- More pixels, clearer image
- Pixel density expressed in dots per inch (DPI)
- Other notable resolution characteristics include dot pitch and refresh rate



*U.S. Department of
Homeland Security*

United States
Secret Service

Dot Pitch

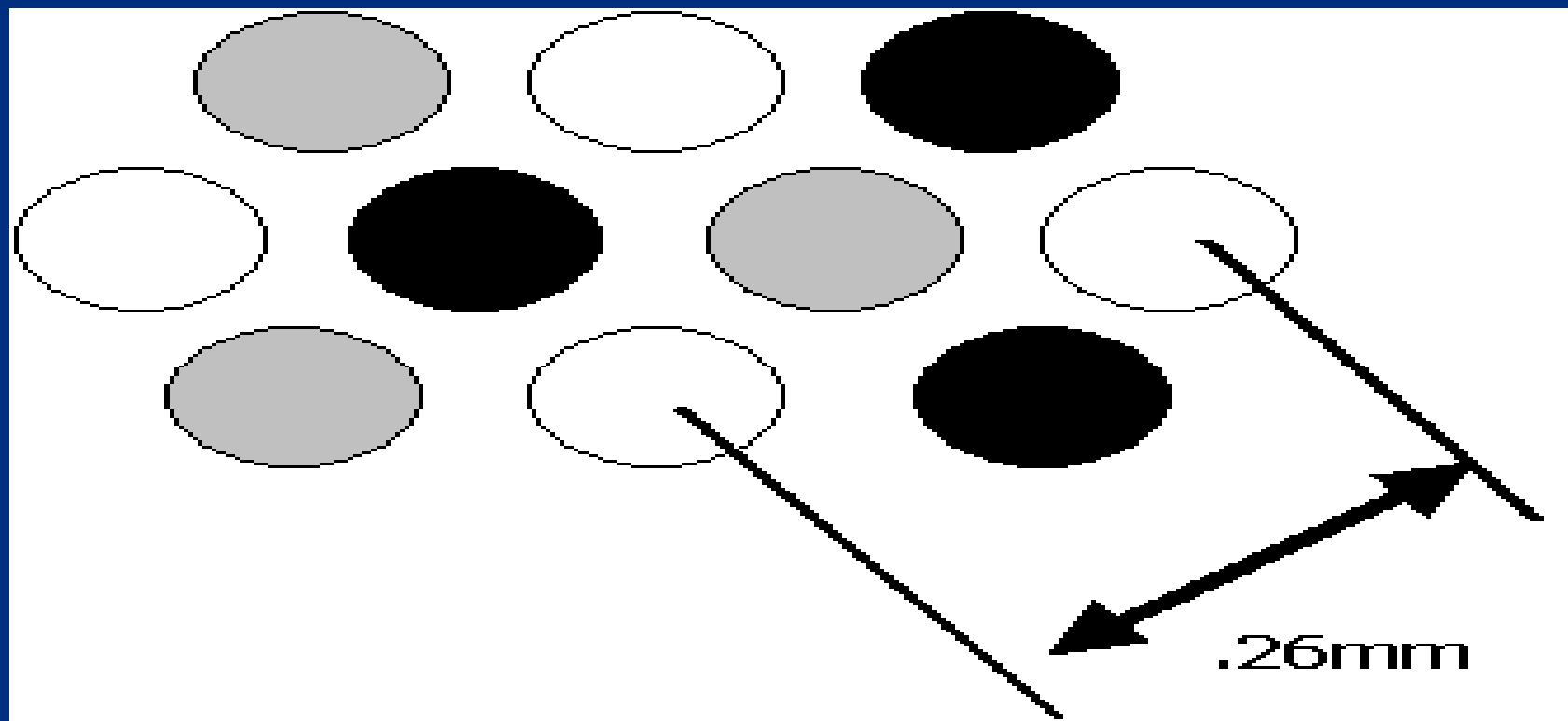
- Dot pitch is distance in millimeters between same color phosphor dots/squares on screen
- Less distance between dots, higher screen resolution
- Smaller dot pitch, greater clarity
- For example, average resolution is approximately .28mm, whereas high resolution is .26mm or less



*U.S. Department of
Homeland Security*

United States
Secret Service

Example of Dot Pitch



*U.S. Department of
Homeland Security*

United States
Secret Service

Refresh Rate

- Speed at which a monitor completes drawing the screen
- Speed is measured in Hz
- Higher the refresh rate, sharper image will be with less screen flicker
- Minimum PC refresh rate is 60 times per second



*U.S. Department of
Homeland Security*

United States
Secret Service

Invar mask

- Perforated nickel-alloy plate inside a CRT (cathode ray tube)
- Perforations contain phosphor 'dots' that glow when stimulated with electrical charge
- Invar mask uses dot geometry to produce an image



*U.S. Department of
Homeland Security*

United States
Secret Service

Aperture grill

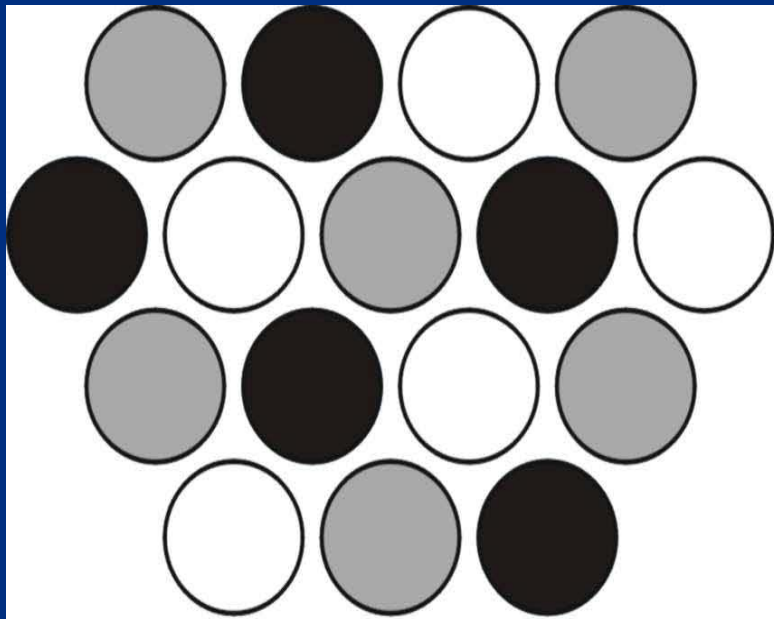
- Screen-embedded metal grillwork
- Grillwork contains phosphor 'squares' that glow when stimulated with electrical charge
- Aperture grill will typically have higher resolution than invar mask and is more durable
- Aperture grill uses rectangular geometry



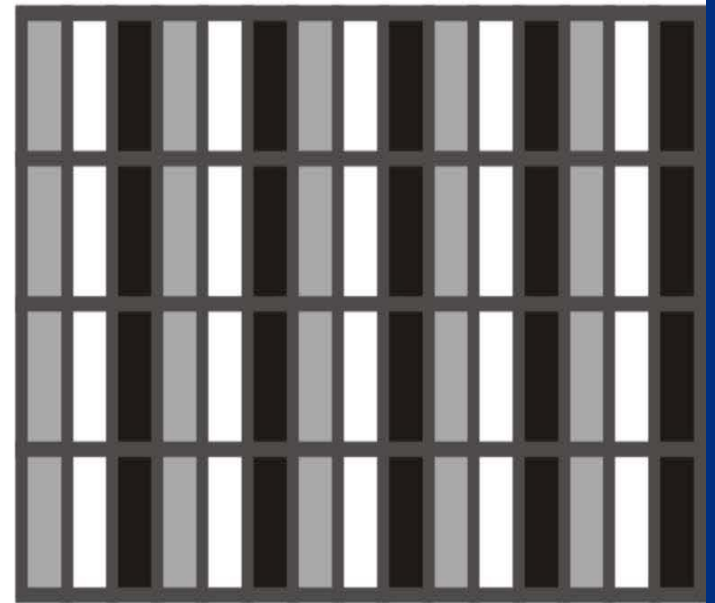
*U.S. Department of
Homeland Security*

United States
Secret Service

Examples of Invar Mask and Aperture Grills



Invar Mask



Aperture Grill



*U.S. Department of
Homeland Security*

United States
Secret Service

Liquid Crystal Display Monitors

- Found in calculators, handheld devices, televisions, PCs, notebook computers
- Produce different colors on screen by using combination of filters and electrically charged liquid crystal cells to filter and change angle of light passing through panel
- Transistors electrically charge crystals
- Number of crystals used is proportional to number of pixels screen can display



*U.S. Department of
Homeland Security*

United States
Secret Service

Liquid Crystal Display Monitors

- Generally use less power than CRT counterparts
- More expensive to manufacture than CRT's and do not have same clarity, contrast ratio, or response time
- Two categories, passive matrix and active matrix LCDs



*U.S. Department of
Homeland Security*

United States
Secret Service

Passive Matrix LCDs

- Passive matrix screen has transistors along edge of screen connected by conductors
- Intersection of conductors forms a pixel
- If screen has 1,024 x 768 pixels, there are 1,024 transistors along horizontal edge and 768 transistors along vertical edge to electrically charge crystals
- Placing transistors along edge of screen, passive matrix LCD monitors are less bright and cheaper to manufacture than active matrix monitors



*U.S. Department of
Homeland Security*

United States
Secret Service

Active Matrix LCDs

- Use the same system of filters and liquid as passive matrix LCDs, but have a transistor for every pixel
- Require a greater number of transistors
- For example, resolution of 1,024 x 768 requires 1,892 transistors for passive matrix monitor and 786,432 transistors for active matrix monitor
- Active matrix monitors provide greater clarity and brightness



*U.S. Department of
Homeland Security*

United States
Secret Service

Organic Light Emitting Diode (OLED) Monitors

- Newer evolution of LCDs
- Do not require a backlight to display pixels, greatly reduces power requirements
- Have an organic substrate that glows when you put an electric current behind it



*U.S. Department of
Homeland Security*

United States
Secret Service

Blurring the Line Between Monitors and Televisions

- Distinction between TVs and monitors greatly eroded
- Many modern televisions, whether LCD or Plasma, feature VGA and DVI inputs to allow direct connections from computers
- Now possible to connect computer directly to 65" LCD display for regular computing



*U.S. Department of
Homeland Security*

United States
Secret Service

MultiTouch Monitors

- Improvement over normal touchscreen monitors, allowing multiple fingers or styluses to interface with screen
- Example is Microsoft's Surface Computer



*U.S. Department of
Homeland Security*

United States
Secret Service

Video Display Adapters

- Video display adapters, also called video cards, are either expansion cards or chipsets on MB that display images on monitor



*U.S. Department of
Homeland Security*

United States
Secret Service

Video Card Components

- Independent BIOS and chipset to control image on screen by first writing data to video RAM
- Video RAM with capacities as high as 1GB
- Video processor (does not depend on the CPU to process signals)
- Optional TV-In/Out connector that redirects display to standard television set or video processing/capturing equipment



*U.S. Department of
Homeland Security*

United States
Secret Service

Example of Video Card



*U.S. Department of
Homeland Security*

United States
Secret Service

Output Devices - Printers

- Device that prints illustrations, charts, or text on paper
- Most prevalent types are dot matrix, ink jet and laser



*U.S. Department of
Homeland Security*

United States
Secret Service

Dot Matrix Printer

- High-speed printer that uses grouping of mechanical pins in the print head
- Text is displayed in rows of dots



*U.S. Department of
Homeland Security*

United States
Secret Service

Ink Jet Printer

- Higher resolution type printer when compared to dot matrix model
- Printing occurs when tiny nozzles spray magnetically directed, ionized ink on paper



*U.S. Department of
Homeland Security*

United States
Secret Service

Laser Printer

- Highest resolution printer
- Print technology uses a toner set and laser tracing to transfer image to paper



*U.S. Department of
Homeland Security*

United States
Secret Service

Input/Output Ports

- Be able to recognize various input/output ports on a PC
- Knowing form and location will ensure proper connections are made

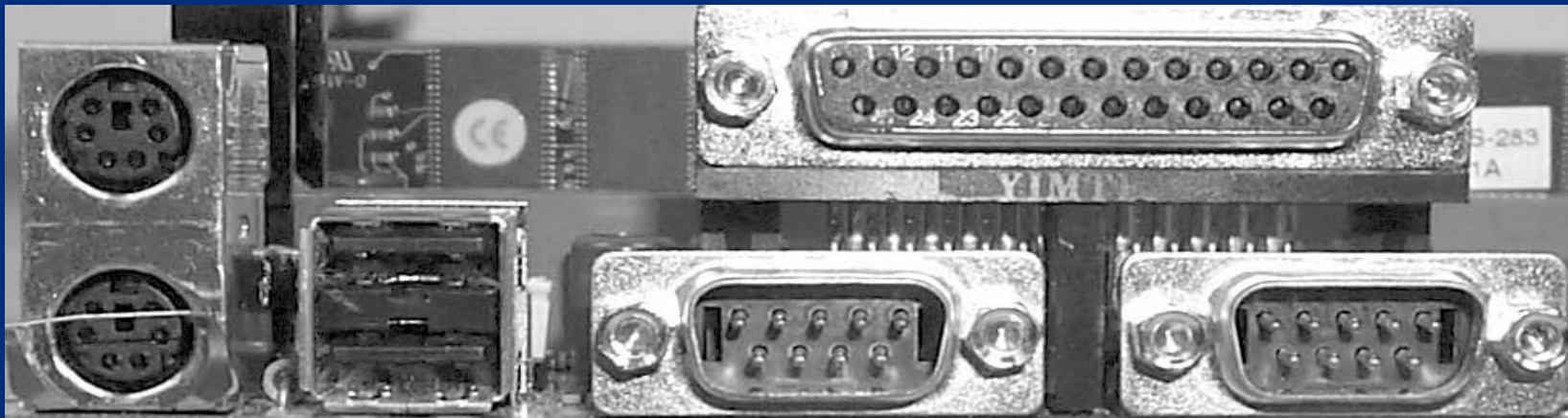


*U.S. Department of
Homeland Security*

United States
Secret Service

Recognizing I/O Ports

Computer Ports



*U.S. Department of
Homeland Security*

United States
Secret Service

Mouse and Keyboard Ports

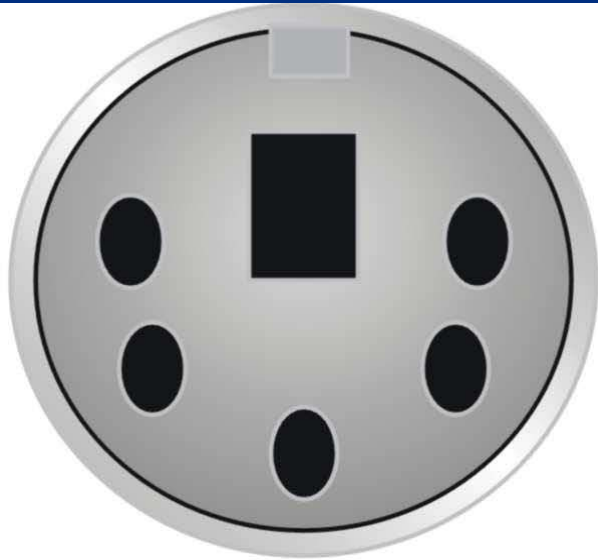
- PS/2 mouse and keyboard use barrel shaped 6-pin mini port
- Ports look exactly alike unless color coded or labeled
- A mouse could require a 9-pin serial or USB port
- Older keyboards connect using a 5-pin barrel-shaped connector, slightly larger than a PS/2 port
- Connectors are found on AT or older MBs



*U.S. Department of
Homeland Security*

United States
Secret Service

PS2 Mouse or Keyboard Port



**AT style 5 pin
keyboard connector**



**PS/2 mouse or
keyboard connector**



*U.S. Department of
Homeland Security*

United States
Secret Service

Serial Ports

- Serial port sends only one bit of data at a time over one wire, typically used to connect older devices to computer such as modems, touchscreens, and proprietary devices
- PCs have maximum of four serial ports referred to as COM 1, COM 2, COM 3, and COM 4
- Ports divided into pairs: COM 1 paired with COM 3 and COM 2 paired with COM 4
- Each pair shares same system resources



*U.S. Department of
Homeland Security*

United States
Secret Service

Serial Ports

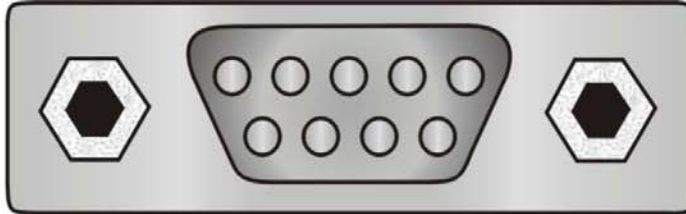
- Ports that comprise a pair cannot be used at the same time
- Example, COM 1 and COM 3 cannot run at same time



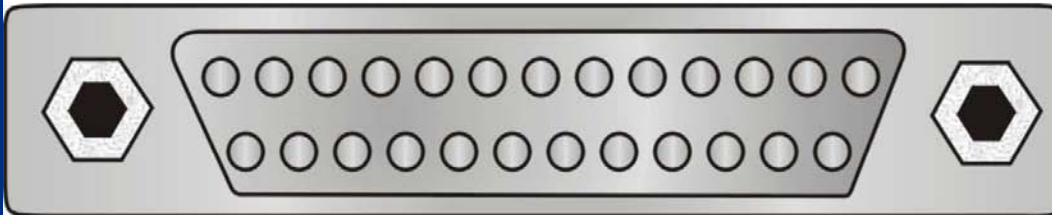
*U.S. Department of
Homeland Security*

United States
Secret Service

9-pin and 25-pin Serial Ports



9-pin male Serial Port



25-pin male Serial Port



*U.S. Department of
Homeland Security*

United States
Secret Service

Parallel Ports

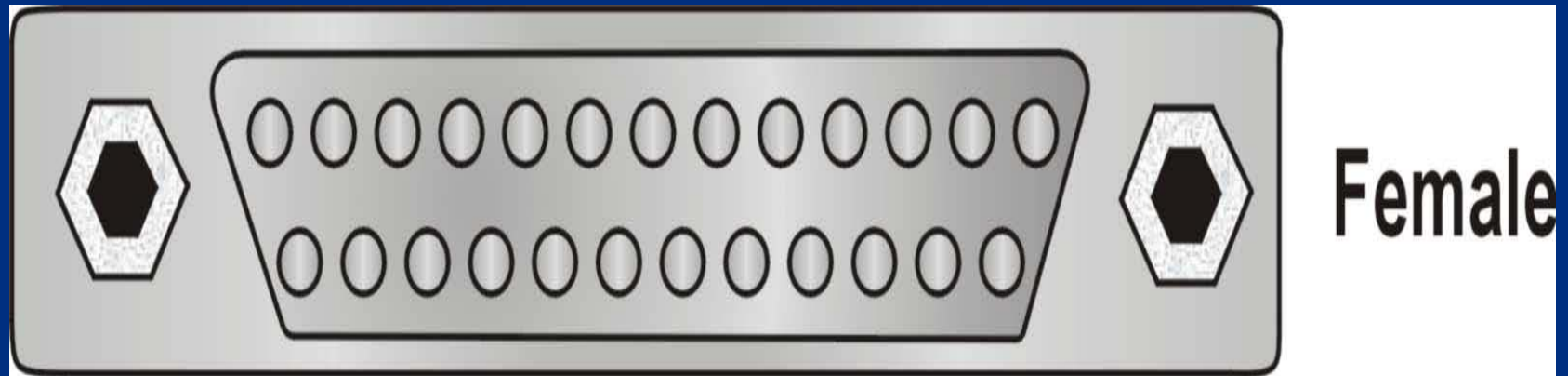
- Most PCs have one parallel port used mainly to connect printer although can be used for certain external drives such as Zip or Jazz
- Parallel port is much faster than the serial port, it can send one byte of data at a time, instead of just a single bit
- Port is either a 25-pin parallel port or a 36-pin Centronics port
- The SCSI-1 parallel port uses a 50-pin Centronics port
- Do not confuse different types of parallel ports



*U.S. Department of
Homeland Security*

United States
Secret Service

Example of Parallel Port



*U.S. Department of
Homeland Security*

United States
Secret Service

Universal serial bus (USB) Port

- USB port enables many different components to be connected to computer sharing the same port using a connection configuration called daisy chain
- Small, flat, rectangular connection that requires a four-wire cable
- Usually found in pairs



*U.S. Department of
Homeland Security*

United States
Secret Service

USB Port

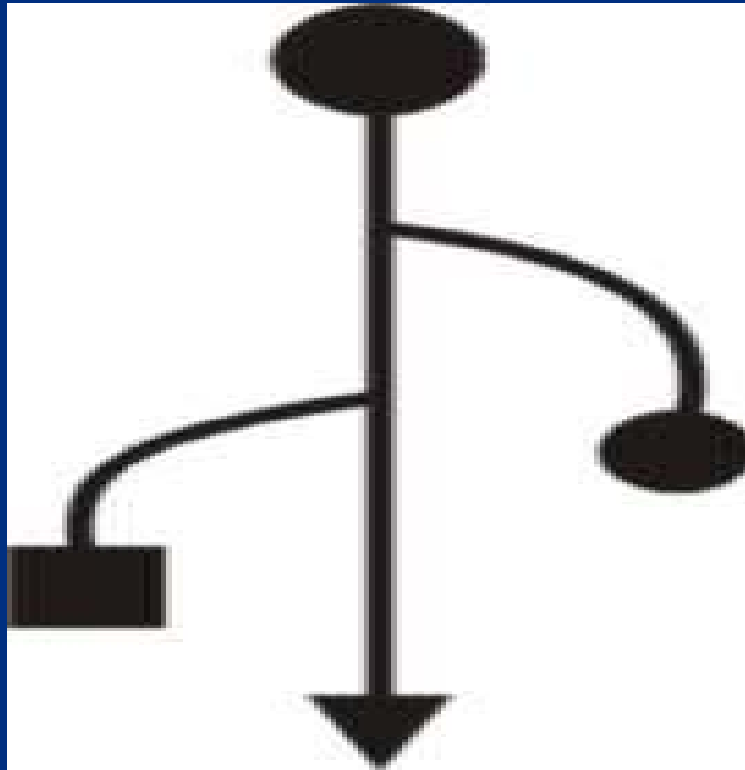
- Most important feature is ability to hot swap or change devices without turning off computer
- In theory, 127 devices can be daisy chained
- Transfer rate of USB 1.1 is 12 Megabit/sec (1.5MB/sec)
- Transfer rate of USB 2.0 is 480 Megabit/sec (60MB/sec)
- Symbol signifying USB port found on back of computer



*U.S. Department of
Homeland Security*

United States
Secret Service

USB Symbol



*U.S. Department of
Homeland Security*

United States
Secret Service

FireWire and i.LINK Ports

- FireWire made by Apple Computers and i.LINK made by Sony are manufacturer brand names for IEEE 1394 ports
- Alternative to USB port, transfer data at higher speed than USB 1.1, generally 50MB/sec
- Either 4-pin or 6-pin connectors with 6-pin port considered the standard
- Allow up to 63 devices to be daisy-chained to one connector

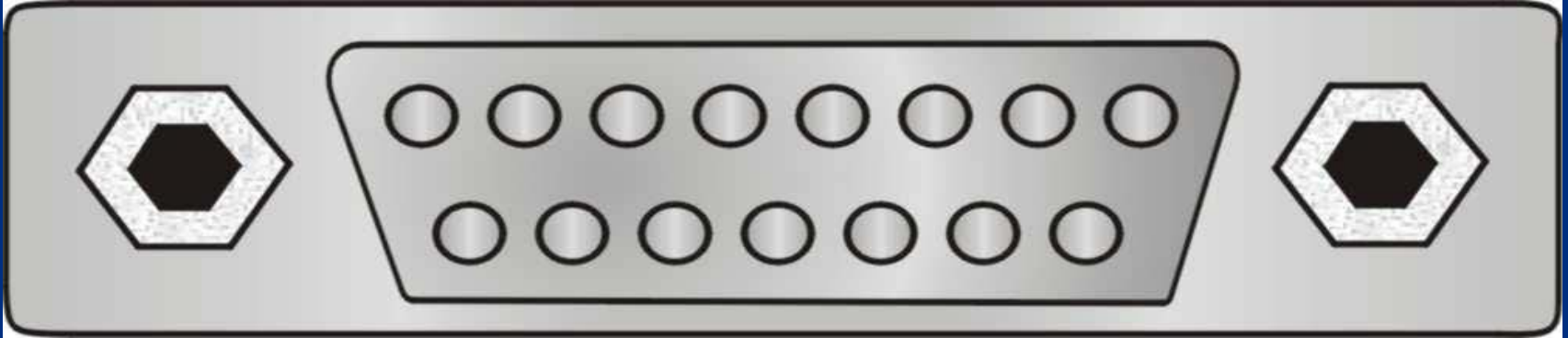


*U.S. Department of
Homeland Security*

United States
Secret Service

Game Controller Port

- Game controller port connects joystick or other type of game controllers to PC
- Port has 15 pins distributed in two rows



*U.S. Department of
Homeland Security*

United States
Secret Service

VGA Video Display Ports

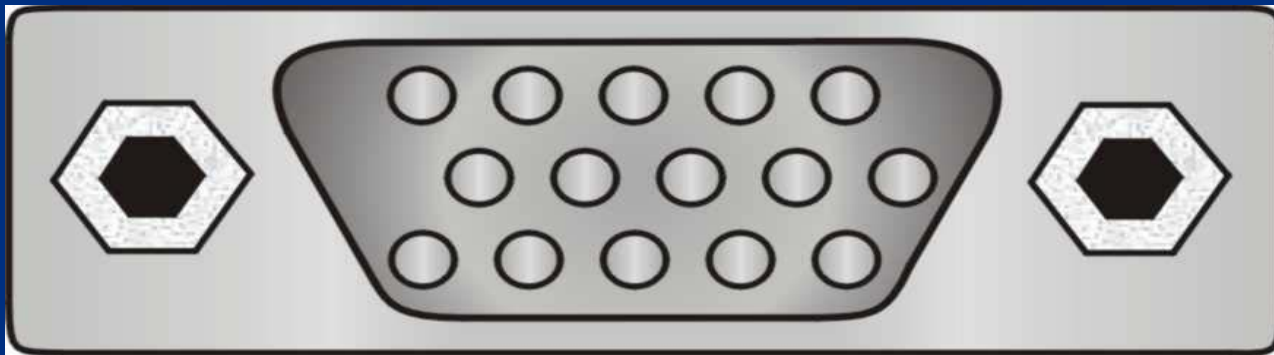
- Video display ports connect monitor to PC
- One of most common video connectors is VGA, which transmits an analog video signal
- VGA has 15 pins distributed in three rows, forming arrow pointing in one direction



*U.S. Department of
Homeland Security*

United States
Secret Service

VGA Video Port

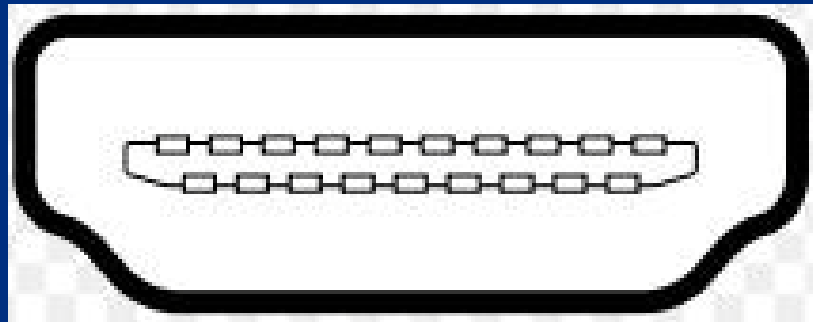


*U.S. Department of
Homeland Security*

United States
Secret Service

HDMI Video Display Ports

- High-definition standard used extensively on televisions and audio/video equipment
- Not commonly found on PC computers, but is supported

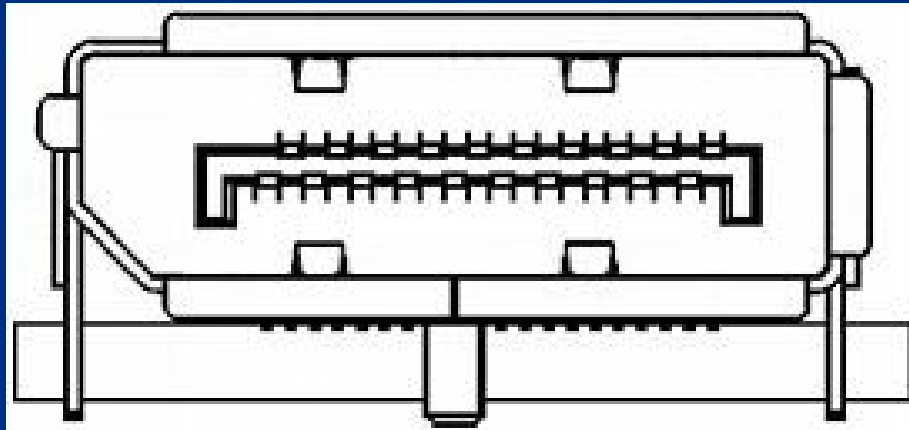


*U.S. Department of
Homeland Security*

United States
Secret Service

DisplayPort Video Display Ports

- Newest standard, designed as a competitor to HDMI
- Supports resolutions up to 2560x1600



*U.S. Department of
Homeland Security*

United States
Secret Service

Sound Ports

- Sound cards and sound chips usually have four round 1/8 inch mini TRS jack ports
- Ports are color-coded and defined as line-in, line-out, microphone, and speaker-out
- Other sound ports may be found on PC including a stereo port, MIDI port or digital audio output port



*U.S. Department of
Homeland Security*

United States
Secret Service

Modems

- Modems handle communications transmitted over telephone lines between computer systems
- Most modern modems have fax capabilities
- PCs are digital devices, telephone system is an analog device



*U.S. Department of
Homeland Security*

United States
Secret Service

Modems

- Modem converts (modulates) the digital code to analog so it can be sent over phone cables
- Modem converts (or demodulates) analog signals to digital code before transmitting data to the PC
- The transmission mode takes two separate forms, asynchronous and synchronous



*U.S. Department of
Homeland Security*

United States
Secret Service

Modems

- Modems have standardized speeds and protocols
- Speed measured in baud or bits per second and varies depending on model
- Standard transmission protocol for modern modems is V.92 protocol that transmits at speed of 56K



*U.S. Department of
Homeland Security*

United States
Secret Service

Modems

- Use two methods to facilitate the transfer of information
- Data Compression – Speeds data transfer
- Error Correction – Allows modem to detect errors in transit and either correct errors or resend data



*U.S. Department of
Homeland Security*

United States
Secret Service

External Modems

- More expensive than internal modems
- Include a separate chassis and power supply
- Readily identifiable by LEDs on front panel
- Connects to serial or USB port, may limit modem from reaching full transmission capabilities



*U.S. Department of
Homeland Security*

United States
Secret Service

Internal Modems

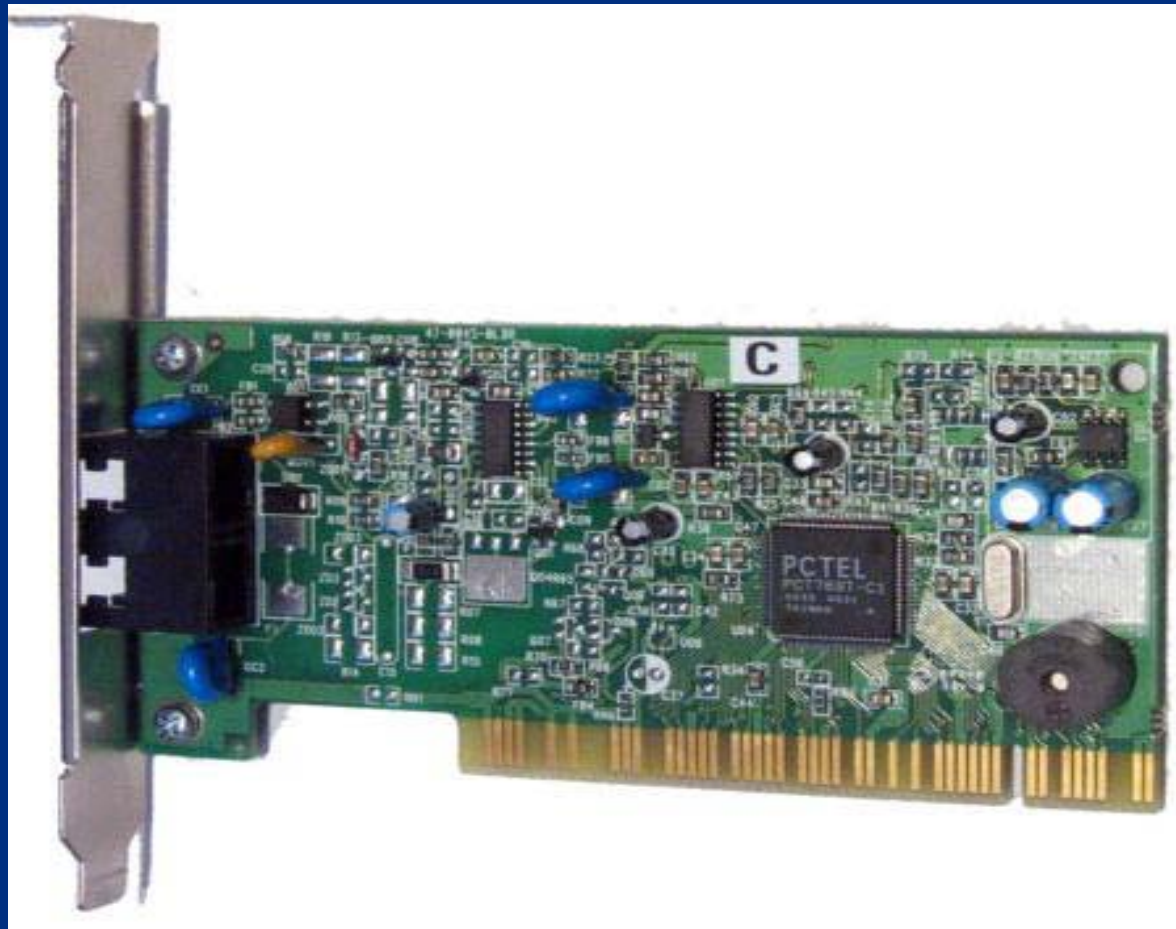
- Internal modems are contained on a PCI or ISA card
- Internal modem will contain separate communications circuitry and is not limited by serial port connection
- Internal modems less expensive than external



*U.S. Department of
Homeland Security*

United States
Secret Service

Example of Internal Modem



*U.S. Department of
Homeland Security*

United States
Secret Service

Caution!

- Never attempt to connect a real analog modem to a multi-line or digital connection
- Voltage requirements are different
- Connection will destroy the modem



*U.S. Department of
Homeland Security*

United States
Secret Service

Winmodems

- Winmodems are internal modems
- Configured by device drivers in operating system rather than by physical jumpers
- Use CPU to process data instead of onboard chip
- Require system drivers to operate, usually work only with Microsoft Windows



*U.S. Department of
Homeland Security*

United States
Secret Service

PC Cards

- *PC cards*, also known as *PCMCIA* (Personal Computer Memory Card International Association) cards
- Metal-encased expansion cards about the size of credit card
- Most often used in laptop computers



U.S. Department of
Homeland Security

United States
Secret Service

Additional Functions Provided

- Fax and modem
- Mini-hard drives
- Network Interface Card (NIC)
- Small Computer System Interface (SCSI) host adapters
- Additional RAM and ROM



*U.S. Department of
Homeland Security*

United States
Secret Service

PC Cards

- PC cards manufactured in four types
- All have same dimensions (3.4 inches by 2.1 inches)
- Differences are in card thickness and functions
- Different card types require different card ports
- Type I cards can be read by a Type II reader
- Type II cards can be read by a Type III reader



*U.S. Department of
Homeland Security*

United States
Secret Service

PC Cards Types

- Type I primarily used to add more memory (3.3 mm thick)
- Type II used for modems and NICs (5 mm thick)
- Type III used to add a mini-hard drive (10.5 mm thick)
- Type IV used to add a high-capacity drive
- Type IV not officially recognized by PCMCIA, there are no official standards for implementation



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 2 – BIOS and System Initialization

- Motherboard Components
- BIOS Information
- The Boot Process
- The Master Boot Record



*U.S. Department of
Homeland Security*

United States
Secret Service

Motherboard Components



*U.S. Department of
Homeland Security*

United States
Secret Service

Motherboard BIOS

- The MB *basic input/output system (BIOS)*, also called system BIOS, considered to be heart of computer
- Controls communications between computer hardware and operating system
- Also referred to as ROM BIOS because the code is contained in a non-volatile, read-only memory (ROM) chip



U.S. Department of
Homeland Security

United States
Secret Service

Motherboard BIOS

- System BIOS contains software called firmware
- *Firmware* provides basic input/output instructions to boot computer and handles several important functions
- Functions include identifying installed hardware, determining boot device, and installing basic drivers for keyboard, video, and disk drives prior to loading OS



U.S. Department of
Homeland Security

United States
Secret Service

Functions of Motherboard BIOS

The four major functions of BIOS are:

- Function 1: Contains and executes POST
- Function 2: Contains CMOS setup program
- Function 3: Executes bootstrap loader
- Function 4: Contains and runs initial boot device drivers



*U.S. Department of
Homeland Security*

United States
Secret Service

Function 1: Contains and executes the power-on-self-test (POST)

- Very generalized, hard-coded diagnostic utility that examines crucial components of system prior to boot procedure
- Tests RAM, video card, keyboard, and disk drive



*U.S. Department of
Homeland Security*

United States
Secret Service

Function 1: Contains and executes the power-on-self-test (POST)

- Finds fatal errors that prevents system from booting and sends the following alerts:
- Series of audio codes or beeps prior to initialization of video
- On-screen text messages after initialization of video
- Numeric codes sent to an internal I/O port address
- Codes can only be read by special PCI or ISA card



*U.S. Department of
Homeland Security*

United States
Secret Service

Function 1: Contains and Executes the Power-On-Self-Test (POST)

- When warnings encountered, either continue to boot, if possible, or enter setup to reconfigure system and resolve error
- Codes can be viewed on BIOS manufacturer's Web site
- System BIOS maintains information about all legacy and Plug and Play devices discovered via POST



*U.S. Department of
Homeland Security*

United States
Secret Service

Function 2: Contains the CMOS Setup Program

- When computer boots, instructions generally found on-screen such as “Press F1 for Setup”
- Setup program run by MB BIOS
- Data generated by Setup stored in separate chip called CMOS
- CMOS stores data such as date and time, device used to boot PC
- Ability to enable or disable many MB functions



*U.S. Department of
Homeland Security*

United States
Secret Service

Function 3: Executes the Bootstrap Loader

- Code that queries CMOS to determine boot device, locates Master Boot Record for device, locates operating system, boots system, gives control of computer to OS
- In short, performs quick check of computer system to ensure that it is ready to accept OS



*U.S. Department of
Homeland Security*

United States
Secret Service

Function 4: Contains, Runs Initial Device Drivers Needed to Boot

- Device driver is a small piece of software code that allows OS to communicate with physical device
- Device drivers loaded by system BIOS are very basic drivers for keyboard, video, and disk drives
- System BIOS contains table of data for several types of disk drives



*U.S. Department of
Homeland Security*

United States
Secret Service

Function 4: Contains, Runs Initial Device Drivers Needed to Boot

- BIOS interrogates drive and uses information in the table to identify the drive and to facilitate access to the drive
- If settings not found through this identification process, drive configuration settings can be entered manually through Setup program



*U.S. Department of
Homeland Security*

United States
Secret Service

The Boot Process

Activity	Description
1. Power on	When Power On button pressed, and power supply reaches working voltage, Power_Good line set to true on microprocessor
2. CPU looks at ROM for basic instructions (BIOS)	When CPU receives power good signal it starts to load the program at memory location 0000h, which is start of BIOS



*U.S. Department of
Homeland Security*

United States
Secret Service

The Boot Process

Activity	Description
3. System BIOS loads	
4. BIOS initiates POST	POST = Power On Self Test



*U.S. Department of
Homeland Security*

United States
Secret Service

The Boot Process

Activity	Description
<p>5. POST checks RAM and Video. If either have a problem, various beep codes sent to speaker.</p> <p><i>From this point forward, errors are reported with text messages displayed on the monitor.</i></p>	<p>Depending on manufacturer, POST error codes vary</p> <p>The following web site outlines many industry error codes: www.bioscentral.com</p>



U.S. Department of
Homeland Security

United States
Secret Service

The Boot Process

Activity	Description
6. When RAM and Video pass POST test, single beep occurs to indicate that diagnostic speaker is working. A malfunctioning speaker will prevent audible beep codes.	You will begin to see text on screen. Rapid numbers flashing indicate in-depth RAM check. Screen will indicate BIOS manufacturer and version number.



*U.S. Department of
Homeland Security*

United States
Secret Service

The Boot Process

Activity	Description
7. POST then checks keyboard.	If an error occurs, a text message generally displays the on-screen
8. The BIOS checks memory location 0472h for the value 1234h which indicates a 'warm start', or that the reset button was pressed.	If this is a warm start BIOS shortens check and load process to only those things necessary to start system, versus full diagnostic check.



*U.S. Department of
Homeland Security*

United States
Secret Service

The Boot Process

Activity	Description
9. CMOS data is compared against new current configuration data. Drives spin, lights flash, and sounds are heard as circuits are tested and prepared for system start-up.	If there is a problem With the CMOS battery, you will get a text message.
10. Finding no major hardware errors, BIOS turns process over to OS boot loader on default boot device.	Boot loader starts, search for Master Boot Record begins.



*U.S. Department of
Homeland Security*

United States
Secret Service

The Boot Process

Activity	Description
<p>11. Boot loader learns boot sequence from (e.g. A: C: CD-ROM, etc.) and looks for Master Boot Record on that device.</p> <p><i>For hard disks, boot loader looks for a partition table. Partition table will have pointer to MBR on primary, active partition.</i></p>	



U.S. Department of
Homeland Security

United States
Secret Service

The Boot Process

Activity	Description
12. MBR contains first file needed to start OS (IO.SYS in Windows 9x, boot.ini in NT).	
13. Process turned over to OS and you see splash screens, etc.	



*U.S. Department of
Homeland Security*

United States
Secret Service

The Master Boot Record (MBR)

- The last thing boot loader does is search for Master Boot Record (MBR) for OS
- Originally found at cylinder 0, head 0, sector 1 of default boot drive
- Default boot drive was usually floppy disk drive
- Today just about any storage device can be configured as default boot device, including USB drives, CD's, DVD's, even network interface



*U.S. Department of
Homeland Security*

United States
Secret Service



*U.S. Department of
Homeland Security*

United States
Secret Service

Module 4 – Operating Systems and Installation



*U.S. Department of
Homeland Security*

United States
Secret Service

You Will Learn . . .

- File System / Operating System Basics
- Software Installation



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 1 - File System/Operating System Basics

- File System Selection
- Operating System Installation
- Operating System Updates



*U.S. Department of
Homeland Security*

United States
Secret Service

Assess Use of Workstation

- Before installation of Windows on your workstation, accurately assess how machine will be used
- Allows for best choices during installation to avoid trouble later



*U.S. Department of
Homeland Security*

United States
Secret Service

File System Options

- Installing Microsoft Windows NT-based operating systems (NT, 2000, XP, 2003, and Vista) provides choice of FAT or NTFS file systems
- Windows Vista does not allow system partition to use FAT file system but additional partitions can use FAT16 and FAT32 file systems



*U.S. Department of
Homeland Security*

United States
Secret Service

NTFS v FAT

- NTFS has several advantages over FAT file systems
- NTFS provides security and better overall performance
- NTFS uses a journaling mechanism which logs disks transactions
- Journaling file systems often do better job at data recovery after power failure



*U.S. Department of
Homeland Security*

United States
Secret Service

FAT v NTFS

- FAT does not provide security but is compatible with older Windows Operating systems such as Windows 95, Windows 98, and Windows ME
- Most USB thumb drives and storage devices are released pre-formatted with FAT
- Allows operating systems such as Linux and Mac OS X to read and write to the device



*U.S. Department of
Homeland Security*

United States
Secret Service

FAT Characteristics

- Each partition or logical drive contains File Allocation Table, or FAT
- FAT manages list of file locations existing on particular drive
- FAT list constantly being updated with new information as files saved, deleted, renamed or moved
- Critical that list stay current and intact to allow operating system to access files



*U.S. Department of
Homeland Security*

United States
Secret Service

FAT Characteristics

- FAT16 used a 16-bit length number to identify clusters on drive
- Limited addressable capacity to 65,526 clusters, 2GB of data
- Use of FAT16 on drives larger than 2GB requires partitioning of drive to use drive's full capacity
- FAT32 uses a 32-bit length number to identify clusters on drive
- Increase allows file system to address approximately 268,400,000 clusters, about 2 terabytes of information



*U.S. Department of
Homeland Security*

United States
Secret Service

NTFS Characteristics

- Windows 2000 and Windows XP can operate in FAT32 or FAT16 environment but default file system is NTFS (New Technology File System)
- NTFS more stable than FAT
- NTFS offers file compression and data encryption
- MS Windows 2000, Windows 2003, and Windows XP Professional support dynamic volumes, allowing partitions to be added or extended without resulting in data loss



*U.S. Department of
Homeland Security*

United States
Secret Service

Converting Partitions

- Windows 2000/XP Disk Management tool allows deletion or modification of partitions and displays general volume information including: file system type, amount of available space and drive's total capacity
- Disk Management also used to convert partition from FAT16/32 to NTFS
- Command prompt can be used to convert partitions to NTFS
- To convert FAT to NTFS type: `convert <drive letter> /fs:ntfs`



*U.S. Department of
Homeland Security*

United States
Secret Service

Converting Partitions

- Partition can also be formatted via My Computer
- FAT partitions can be converted to NTFS while preserving data
- NTFS partitions cannot be converted to either FAT file systems



*U.S. Department of
Homeland Security*

United States
Secret Service

MFT (Master File Table)

- NTFS utilizes the MFT (Master File Table) to track files and associated locations on NTFS volume
- MFT is similar to FAT in that it maps location of directories and folders and is updated whenever a file is accessed, changed, deleted or added
- FAT can be thought of as a static fixed-sized chart that cannot change in size
- MFT is dynamic, a relational database that can grow in size if necessary



*U.S. Department of
Homeland Security*

United States
Secret Service

MFT (Master File Table)

- MFT created when drive (or volume) formatted with NTFS
- Certain amount of contiguous space reserved for MFT expansion, sometimes called “MFT Zone”
- Initially, zone approximately 12 percent of total volume capacity
- Most NTFS volumes no larger than 2 terabytes in size, but dynamic nature of MFT allows volume to reach 16 Exabyte's, equivalent to approximately 16,000,000 terabytes in capacity!



*U.S. Department of
Homeland Security*

United States
Secret Service

File Systems for Operating Systems

Operating System	Type of Primary File System	Characteristics of File System
DOS	FAT16	<ul style="list-style-type: none">• Limited to 2GB partitions
Windows for Workgroups	FAT16 w/ limited VFAT	<ul style="list-style-type: none">• 32-bit file access
Windows 95a	VFAT	<ul style="list-style-type: none">• 32-bit file access• Supports long file names



*U.S. Department of
Homeland Security*

United States
Secret Service

File Systems for Operating Systems

Operating System	Type of Primary File System	Characteristics of File System
Windows 95b (OSR2), Windows 98, Windows ME	FAT32	<ul style="list-style-type: none">• Supports larger disk capacity up to 2TB• Uses smaller cluster sizes for more efficient storage• Windows 2000 supports FAT32 with disk volumes up to 32GB



*U.S. Department of
Homeland Security*

United States
Secret Service

File Systems for Operating Systems

Operating System	Type of Primary File System	Characteristics of File System
Windows NT	NTFS	<ul style="list-style-type: none">• Improved reliability, and fault tolerance• Security and Access Control• Supports long file names• Supports larger sized partitions, up to 16 Exabytes



*U.S. Department of
Homeland Security*

United States
Secret Service

File Systems for Operating Systems

Operating System	File System	Characteristics of File System
Windows 2000, XP	NTFS	<ul style="list-style-type: none">• Improved Security• Internal Data Encryption• Disk Quotas
Linux (kernel versions prior to 2.4.16)	Ext2fs	<ul style="list-style-type: none">• Security and Access Control• Supports partitions up to 4TB• Supports long file names
Linux	Ext3fs	<ul style="list-style-type: none">• Faster than ext2fs• Greater data control



*U.S. Department of
Homeland Security*

United States
Secret Service

Patching

- Install Operating System patches and critical updates on regular basis
- Use Windows Update to choose Express or Custom settings
- Express Settings installs all high priority updates
- Custom settings will allow user to choose updates to install
- Alternatively, use Windows Automatic Update, during middle of night, every night



*U.S. Department of
Homeland Security*

United States
Secret Service

Danger of Automatic Patching

- By default, Windows XP will automatically download and install new patches on weekly basis
- Drawback, if critical update is released, computer will automatically install and reboot, closing all open applications during process
- Potential exists for loss of data if open files have not been saved



*U.S. Department of
Homeland Security*

United States
Secret Service

Disable Auto Patching

- To disable setting, select Start > Control Panel > System Properties
- Locate and select the tab for “Automatic Updates”
- Recommended value for workstation is “Download updates for me, but let me choose when to install them”
- With option set, update icon will be in system tray and notify when new updates have been downloaded
- Apply updates when safe to do so



*U.S. Department of
Homeland Security*

United States
Secret Service

Operating System Updates

- Use the Step/Action procedure in your student book to install current System Updates



*U.S. Department of
Homeland Security*

United States
Secret Service

Module 5 – Introduction to Networks



*U.S. Department of
Homeland Security*

United States
Secret Service

You Will Learn . . .

- Network Basics
- Network Technologies
- Network Topologies
- Network Architecture
- The OSI Model



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 1 – Network Basics

- Introduction to Networks
- Network Types
- Network Categories



*U.S. Department of
Homeland Security*

United States
Secret Service

Main purposes of a Network

- Transfer data
- Share hardware and system resources
- Communicate via the Internet



*U.S. Department of
Homeland Security*

United States
Secret Service

IEEE 802 Standards

- February 1980, members of Institute of Electrical and Electronic Engineers (IEEE) develop data communications standards
- IEEE 802 standard governs Local Area Network (LAN) and Wide Area Network (WAN) communications
- Specifications for physical network devices, such as network interface cards (NICs), cables, routers, bridges, and access methods, ways data flows through physical network



*U.S. Department of
Homeland Security*

United States
Secret Service

IEEE 802 Standards

IEEE 802 Standard	Description
802.1	High Level Interface
802.2	Spanning Tree
802.3	Logical Link Control (LLC)
802.4	Token Bus Networks
802.5	Token Ring Networks
802.6	Metropolitan Area Networks (MAN)



*U.S. Department of
Homeland Security*

United States
Secret Service

IEEE 802 Standards

IEEE 802 Standard	Description
802.7	Broadband Technical Advisory Group
802.8	Fiber Optic Technical Advisory Group
802.9	Integrated Voice and Data Network
802.10	Network Security
802.11	Wireless LANs



*U.S. Department of
Homeland Security*

United States
Secret Service

IEEE 802.3 and 802.5 Standards

- IEEE 802.3 sets standards for today's Ethernet networks
- IEEE 802.5 governs Token Ring standards
- Ethernet most common architecture found in modern networks
- Token Ring was standard for government networks for many years



*U.S. Department of
Homeland Security*

United States
Secret Service

IEEE 802.11 Standards

- The IEEE 802.11 (a/b/g/n) defines all aspects of radio frequency wireless networking
- Wireless networking uses technology in radio frequency transmissions to send network packets across airwaves



*U.S. Department of
Homeland Security*

United States
Secret Service

IEEE 802.11e Standards

- Enhancement to improve quality of service for 802.11a and 802.11g standards
- Improves quality of multimedia performance through wireless networks
- Uses TDMA (time division multiple access) technology



*U.S. Department of
Homeland Security*

United States
Secret Service

TDMA

- Divides radio frequencies into three time slots to increase amount of available bandwidth that can carry data
- Adds error-correcting mechanisms, reduces time delays often experienced when streaming video
- Offers more reliable medium for multimedia-based transfers such as full-motion video, high fidelity audio, and VoIP



*U.S. Department of
Homeland Security*

United States
Secret Service

IEEE 802.16 Standards

- Not shown in list on earlier slide
- Emerging standard for high speed wireless broadband
- Intended to be compatible with 802.11 standards



*U.S. Department of
Homeland Security*

United States
Secret Service

Networks

- Can be simple as two PCs joined together with single cable or complex as thousands of PCs joined through complicated matrix of routers, switches, public and private infrastructures, multiple cable types, and access methods
- Regardless of simplicity or complexity, all networks provide ability to share data or resources between at least two networked devices



*U.S. Department of
Homeland Security*

United States
Secret Service

Local Area Networks (LANs)

- Connect computers and peripherals to shared transmission medium, such as coaxial cable or a multi-port hub
- Generally span small area within building or several buildings in close proximity
- Each computer can access files and share devices, such as printers and scanners, anywhere on LAN



*U.S. Department of
Homeland Security*

United States
Secret Service

Local Area Networks (LANs)

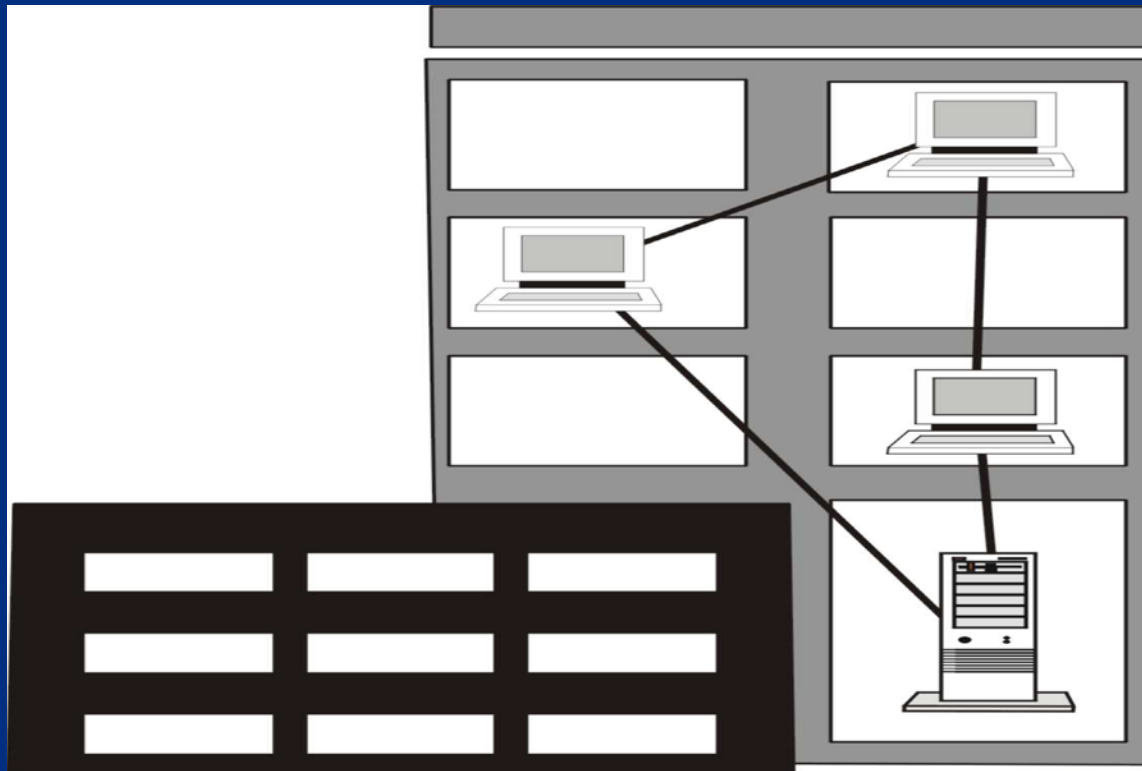
- Size and distance limitations
- Large networks not suited to single LAN design, performance diminishes as more workstations attempt to access network cable
- Many ways to compensate for negative impact of adding numerous workstations to large LANs



*U.S. Department of
Homeland Security*

United States
Secret Service

LAN Example Within a Building



*U.S. Department of
Homeland Security*

United States
Secret Service

Wide Area Networks (WANs)

- Used to move information greater distances beyond LAN's capabilities
- Provides long-distance, internal network that links LANs located in different parts of a city, country, or globe
- Links individual LANs using fiber optic, copper wire, or wireless transmission medias



*U.S. Department of
Homeland Security*

United States
Secret Service

Types of WANs

- Metropolitan Area Network (MAN) – Data network spans all sites within metropolitan area
- Enterprise Network – Connects all LANs of large, single organization and can cross regional boundaries
- Global Network – Data network that spans globe crossing multiple national boundaries
 - May include networks of several organizations



*U.S. Department of
Homeland Security*

United States
Secret Service

WAN

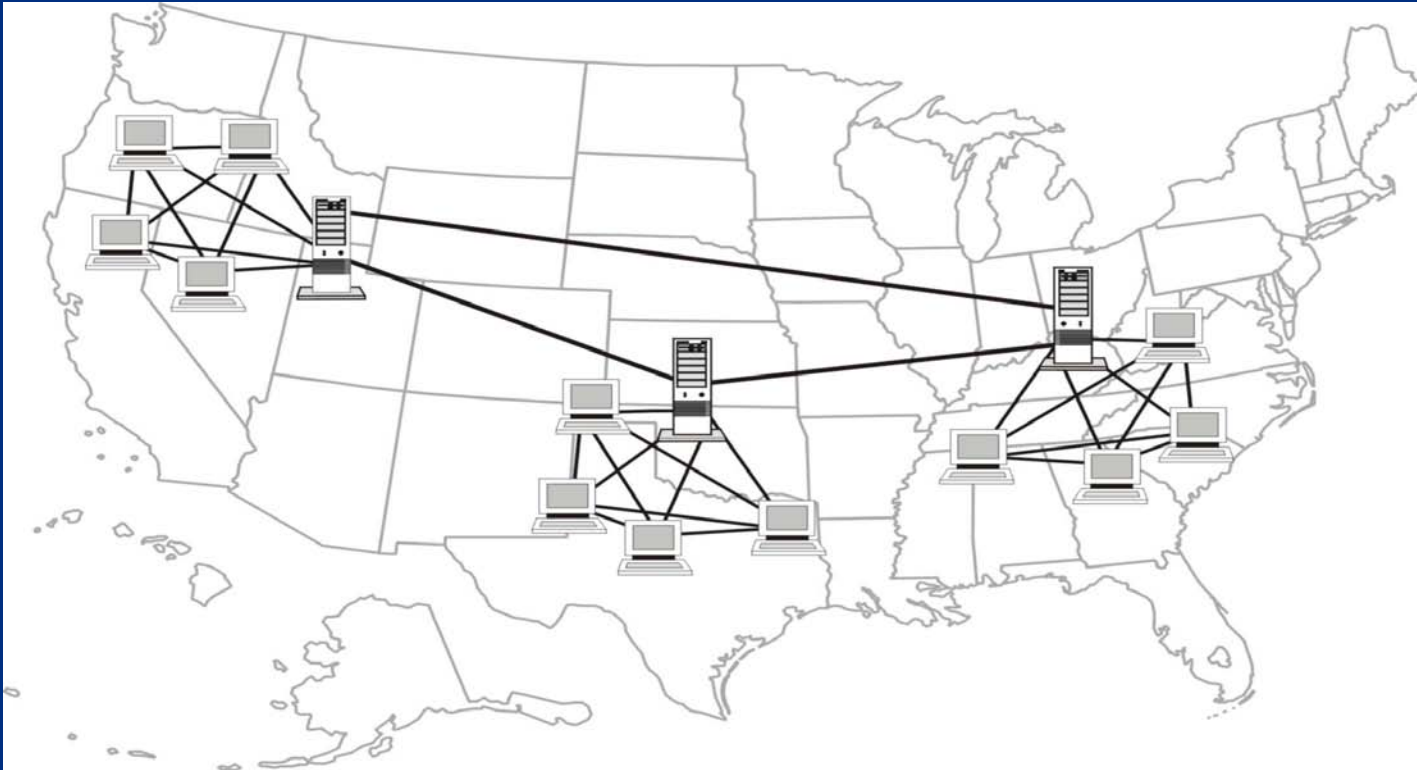
- Composed of interconnected LANs
- In general, can have slower transmission rate than LAN
 - LAN can have transmission rate of 100 Mbps but medium that connects to other LANs on WAN may only transmit at 64 Kbps per channel



*U.S. Department of
Homeland Security*

United States
Secret Service

WAN Illustration



*U.S. Department of
Homeland Security*

United States
Secret Service

Internet

- Massive web of interconnected networks spanning globe
- Community of government agencies, private organizations, and educational institutions
- No one entity owns Internet
- Nearly every organization uses it to communicate, share data, conduct research, and share resources such as data management and storage
- Individuals rely on Internet for e-mail, news services, etc.



*U.S. Department of
Homeland Security*

United States
Secret Service

Internet

- Represents largest repository of electronic information
- Internet service providers (ISP) control connectivity of Internet
- ISPs provide access for fee
- Individuals pay fee to companies like America Online and receive username, password, software, and access phone number
- ISPs provide large organizations means to connect their networks to Internet



*U.S. Department of
Homeland Security*

United States
Secret Service

Intranet and Extranet

- Many businesses and organizations maintain an *intranet*, or internal Web site to communicate with employees or group members
- Intranet access limited to those granted permission to use site
- Intranet provides Internet-like network inside organization to include Web page hosting and use of Web page browsers to access internal data
- *Extranets* established when organization wants to extend intranet to business partners or others outside company



U.S. Department of
Homeland Security

United States
Secret Service

Circuit-switched Networks

- All components physically connected in circuit-switched network using wire, cable, or other transmission media
- Type of network can be compared to telephone system whereby communication requires dedicated communication channel and constant connection
- Integrated Services Digital Network (ISDN), telecommunications standard for providing digital service using telephone networks, example of circuit-switched services



*U.S. Department of
Homeland Security*

United States
Secret Service

Circuit-switched Networks

- Circuit-switched equipment uses digital signaling to establish connection, transfer data on channel, and terminate connection
- All data traverses network on same pathway
- Data divided into small sections called packets
- Only initial packet needs address information as all subsequent transmitted data follows same continuous path



*U.S. Department of
Homeland Security*

United States
Secret Service

Circuit-switched Networks

- If connection broken, communication must start over as remaining packets are not addressed and unable to reach destination
- Referred to as connection-oriented



*U.S. Department of
Homeland Security*

United States
Secret Service

Packet-switched Networks

- Users share network and connections established with variety of possible endpoints
- Like circuit-switched networks, data divided into packets before being transferred across network
- Unlike circuit-switched networks, each packet carries addressing information, packets can be delivered out of order
- Receiving device arranges packets in correct order



*U.S. Department of
Homeland Security*

United States
Secret Service

Packet-switched Networks

- Data can still be transferred in event of interruption or link failure
- Examples of network model include Asynchronous Transfer Mode (ATM), frame relay, symmetric multiprocessing system (SMP), and X.25
- If connection broken, communication does not start over as remaining packets each contain address information and are able to reach destination via any functioning route
- Referred to as connectionless



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 2 – Network Technologies

- Introducing Network Technologies



*U.S. Department of
Homeland Security*

United States
Secret Service

Network Technologies

- Data transferred across a network using several network technologies
- Two most common are broadcast and point-to-point



*U.S. Department of
Homeland Security*

United States
Secret Service

Broadcast Networking

- Most common type of modern network
- Uses broadcast technology to communicate across shared media; copper, optic fiber, or radio waves
- Network devices compete for use of shared media by sensing when available for transmission
- Sensing opportunity to transmit, workstation transmits packets intended for network device such as printer
- As workstation transmits, packets are broadcasted to all devices sharing media



*U.S. Department of
Homeland Security*

United States
Secret Service

Broadcast Networking

- Broadcast packets received by network devices either accepted or ignored, based upon destination address embedded in packet
- Common for multiple transmissions to occur at same time
- Since transmissions are sent to all devices on shared media, transmitted packets often collide, resulting in loss of packets



*U.S. Department of
Homeland Security*

United States
Secret Service

Broadcast Networking

- When packets collide and not received by intended recipient, they are retransmitted
- Because collisions are common in broadcast network, term collision domain frequently used to refer to broadcast network
- Ethernet is example of broadcast network



*U.S. Department of
Homeland Security*

United States
Secret Service

CSMA/CD and CSMA/CA

- Broadcast network access methods
- Carrier Sense Multiple Access/Collision Detection (CSMA/CD)
- Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)



*U.S. Department of
Homeland Security*

United States
Secret Service

CSMA/CD

- Set of rules to determine how network devices connected to broadcast network can access network to send data
- Network cable can only transmit one communication at a time
- Computers on network must compete for access to network
- Designed to avoid repeated packet collisions
- After collision, sending devices are assigned random time to wait before resending packets
- Rare for two sending devices to create two collisions in a row



*U.S. Department of
Homeland Security*

United States
Secret Service

Point-to-Point Networking

- Type of network provides connections between two network devices, sender and receiver
- Data only travels between two connections, not broadcasted to other devices
- Token Ring is example of point-to-point network



*U.S. Department of
Homeland Security*

United States
Secret Service

Token Passing

- Access method used by point-to-point networks
- Computers arranged in a circle or closed loop
- Token travels around network transmitting one packet of information at a time
- Computers connected to network wait for empty token and attach message for transmission
- Rather than competing for access, each network device in turn has fair chance to “grab” empty token for use



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 3 – Network Topologies

- Topologies Defined



*U.S. Department of
Homeland Security*

United States
Secret Service

Physical Topology

- Physical layout of workstations, servers, cabling, printers, and other devices
- Cables and connections in physical topology are called the network transmission media
- Implements one of network technologies mentioned earlier, broadcast or point-to-point



*U.S. Department of
Homeland Security*

United States
Secret Service

Logical Topology

- The way data flows through network
- Dictated by technology implemented



*U.S. Department of
Homeland Security*

United States
Secret Service

Six main Topologies

- Bus
- Star
- Tree
- Ring
- Star-Wired Ring
- Mesh



*U.S. Department of
Homeland Security*

United States
Secret Service

Bus Topology

- Least complex configuration of topologies and uses least amount of cable
- Workstations connected along single, straight line of coaxial cable
- Signal broadcast to all devices connected to cable using CSMA/CD traveling down cable until accepted at intended destination
- When data sent, each device checks destination address of data as it passes, ignoring data if intended for another device



*U.S. Department of
Homeland Security*

United States
Secret Service

Bus Topology

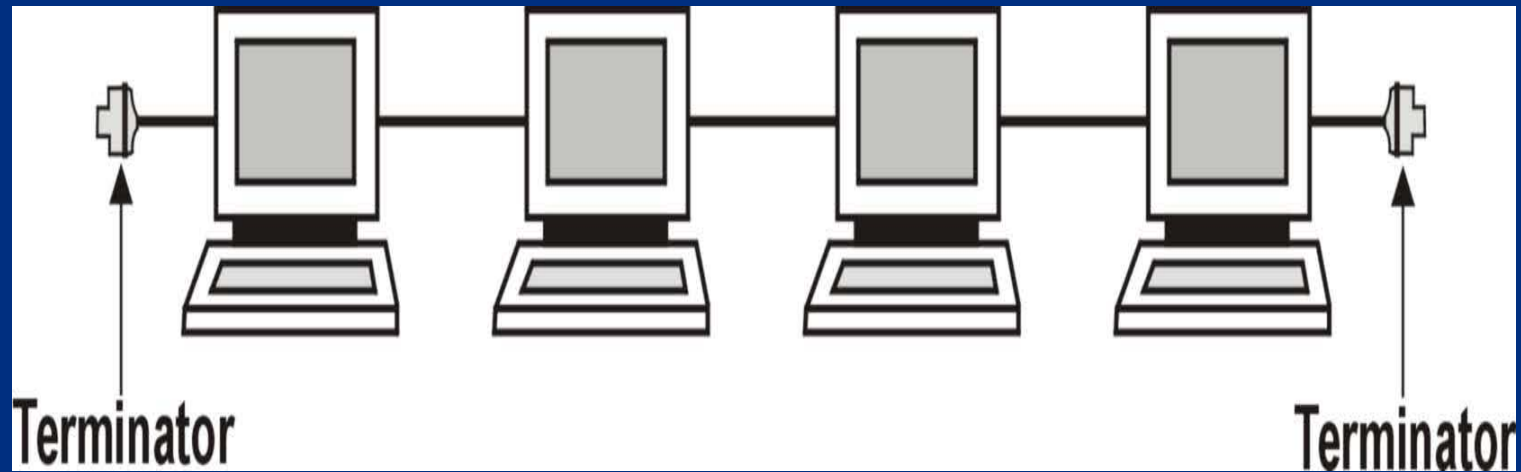
- Bus network requires terminator connected to both ends of line
- Terminators prevent signals from bouncing endlessly back and forth along cable causing packet storm, which will render network inoperable
- Bus networks easily set up because they only require cable adapters to join cable to network card and terminators at each end
- Major disadvantage is broken connection anywhere along cable causes entire network to go down



*U.S. Department of
Homeland Security*

United States
Secret Service

Bus Network Topology



*U.S. Department of
Homeland Security*

United States
Secret Service

Star Topology

- All network devices attached to central hub
- Topology resembles spokes that radiate from hub of a wheel
- Communication among devices on network handled by cabling between device and hub
- All data passes first through hub
- Hub broadcasts data to all devices connected to hub's ports



*U.S. Department of
Homeland Security*

United States
Secret Service

Star Topology

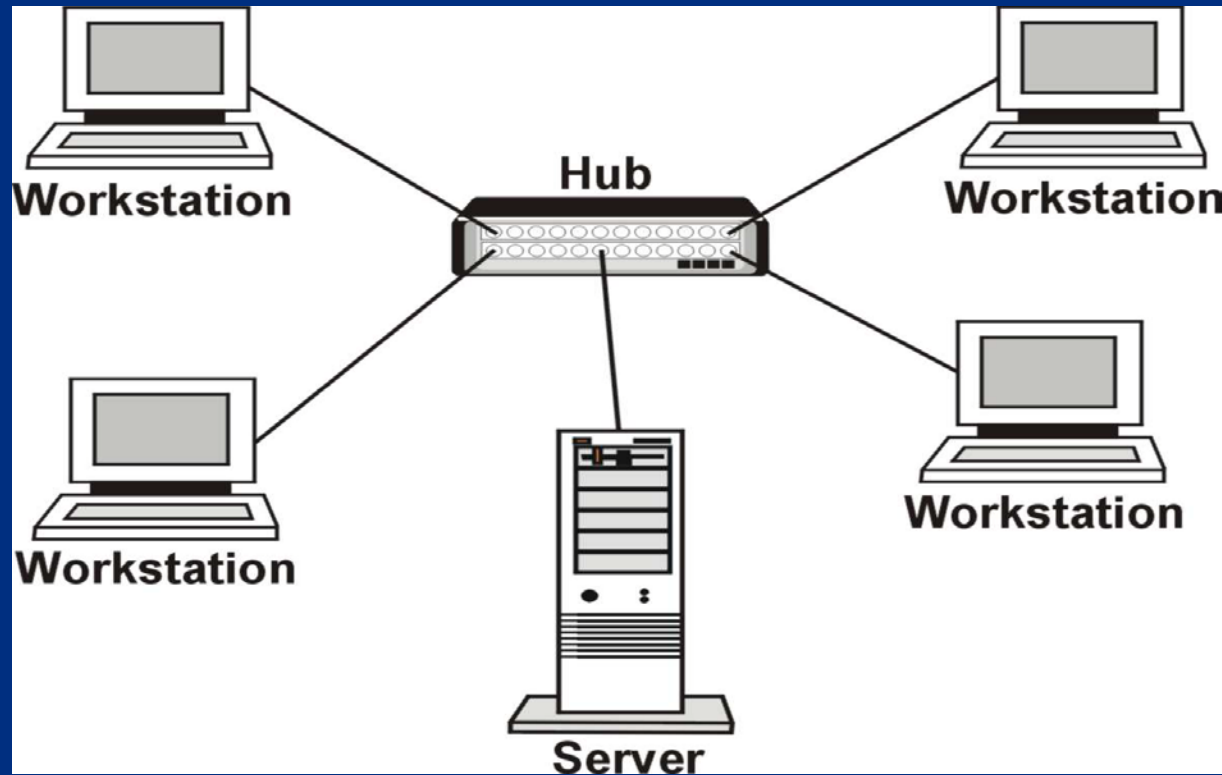
- Data flows on direct line between device and hub, making it easy to troubleshoot problems
- Break in single cable in network will not affect rest of network
- Hub will simply ignore port from which PC is disconnected



*U.S. Department of
Homeland Security*

United States
Secret Service

Star Topology



*U.S. Department of
Homeland Security*

United States
Secret Service

Star Topology

- Star topology is physical star and logical bus
- Devices are connected to central point resembling graphic on previous slide
- Underlying technology is broadcast
- Devices still compete using CSMA/CD just like bus topology



*U.S. Department of
Homeland Security*

United States
Secret Service

Advantages of Star Topology

- Support different types of cabling
- Add/remove nodes easily
- Can be moved easily
- Can easily identify faulty node or connection



*U.S. Department of
Homeland Security*

United States
Secret Service

Disadvantages of Star Topology

- Requires lot of cabling
- Hub can be single point of failure causing entire network to go down



*U.S. Department of
Homeland Security*

United States
Secret Service

Tree Topology

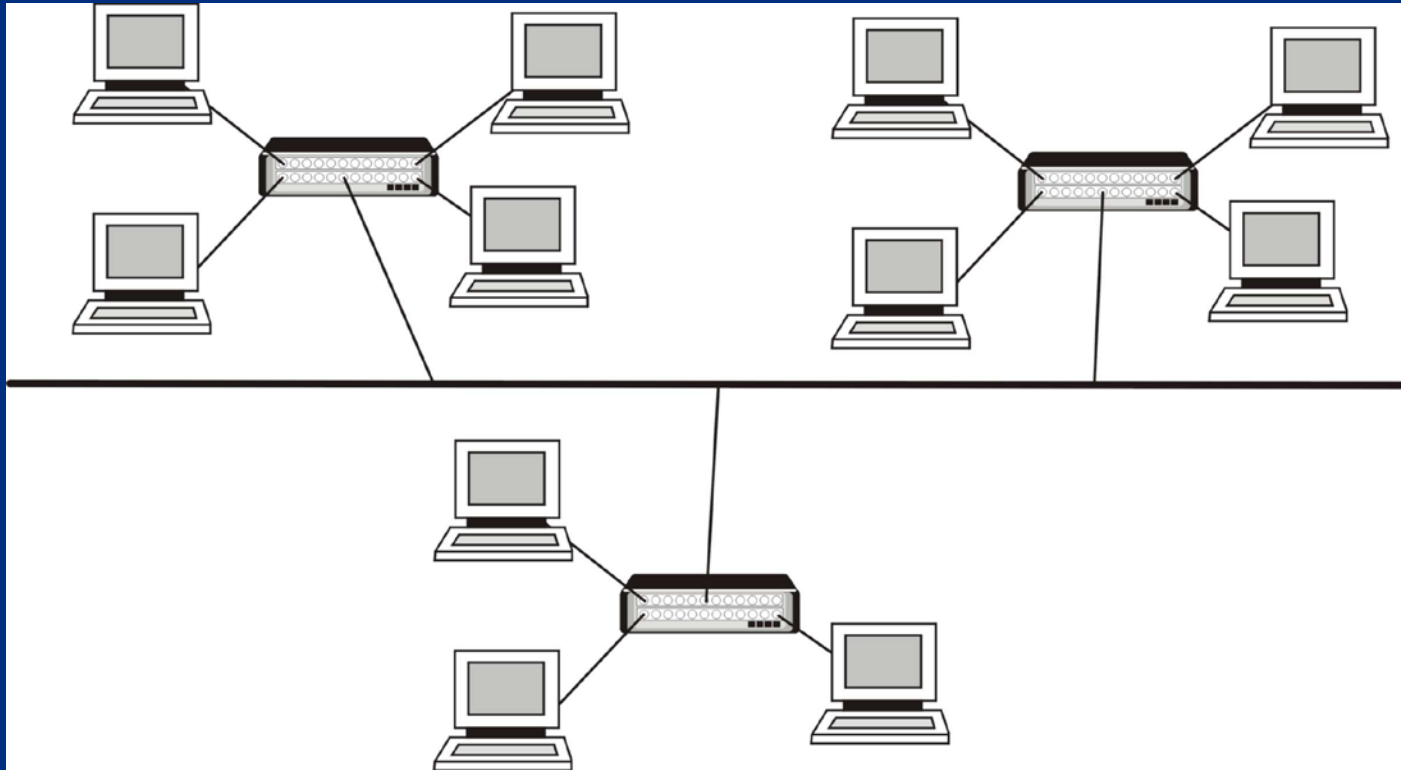
- Tree network is hybrid of star and bus topologies
- Network's physical layout uses distributed bus or branching topology to connect combination of bus and star segments
- Logical topology of tree network transmits data in broadcast form like bus network
- Physical topology combines features of both bus and star layouts



*U.S. Department of
Homeland Security*

United States
Secret Service

Tree Network Topology



*U.S. Department of
Homeland Security*

United States
Secret Service

Advantages of Tree Topology

- Easy to relocate
- Easy to add/remove nodes



*U.S. Department of
Homeland Security*

United States
Secret Service

Disadvantages of Tree Topology

- Access and performance declines if tree network is too large
- Entire network disabled from point of failure on down



*U.S. Department of
Homeland Security*

United States
Secret Service

Ring Topology

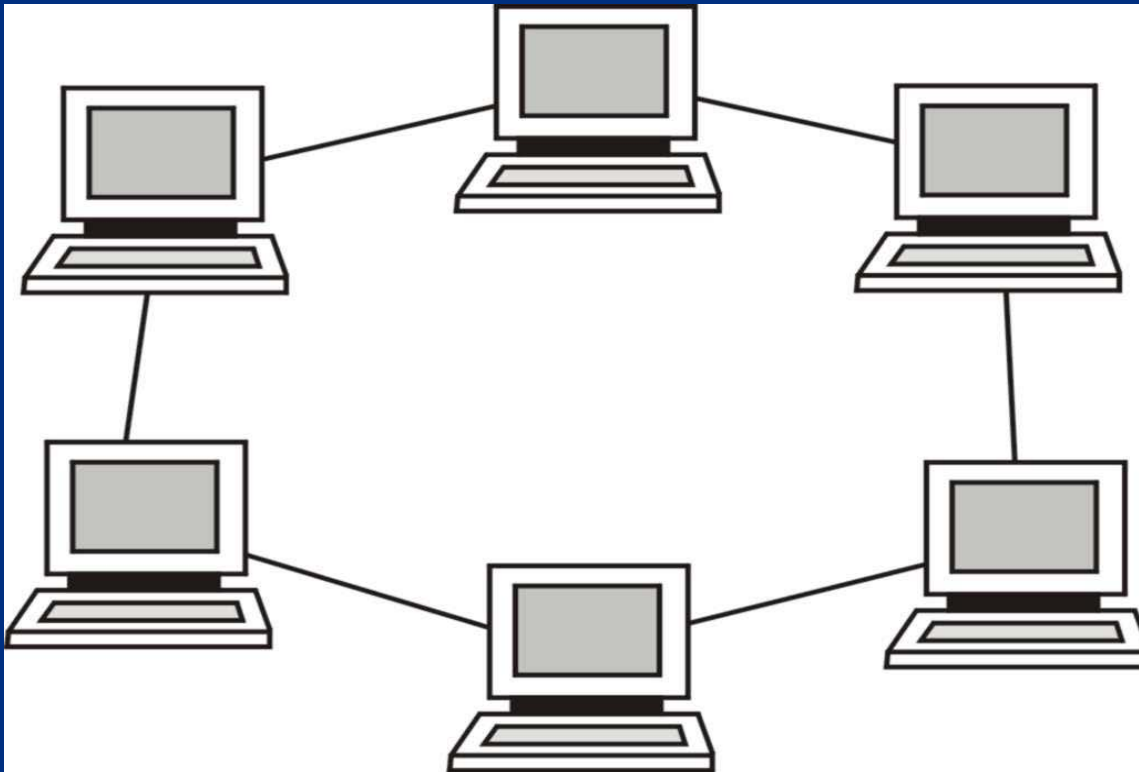
- All devices linked together in closed loop or ring
- Twisted-pair cabling generally used to connect computers
- Uses token passing technology to transmit packets
- Data broadcast only between sending and receiving devices
- Break in cabling or malfunction of NIC can disrupt entire network
- Topology rarely used today



*U.S. Department of
Homeland Security*

United States
Secret Service

Ring Network Topology



*U.S. Department of
Homeland Security*

United States
Secret Service

Star-Wired Ring Network

- Physical topology resembles star physical topology and uses cabling that connects computers to multi-station access unit (MAU)
- Data signals flow in one direction through network using ring logical topology (point-to-point / token passing)
- Main advantage of star-wired ring network is ease of troubleshooting
- Disconnect between device and MAU, affects only that device, rest of network continues to function



*U.S. Department of
Homeland Security*

United States
Secret Service

Mesh Network Topology

- Direct, point-to-point connection made between each network device
- Mesh networks often used to connect LANs to create WAN
- Mesh topology works well for WANs because connections between various locations can be via Internet, satellite, or other high-speed connection



*U.S. Department of
Homeland Security*

United States
Secret Service

Mesh Network Topology

- Advantages of mesh topology include, multiple routes to each host and no single point of failure
- Main disadvantage is expense
- Mesh describes physical topology
- Mesh networks can contain logical point-to-point, broadcast, or combination of both



*U.S. Department of
Homeland Security*

United States
Secret Service

Topology Summary

- Topology defines both physical characteristics of network and the way data flows through network



*U.S. Department of
Homeland Security*

United States
Secret Service



Lesson 4 – Network Architecture

- Introduction to Network Architecture
- Ethernet
- Token Ring
- Fiber Distributed Data Interface (FDDI)
- Asynchronous Transfer Mode
- Broadband



*U.S. Department of
Homeland Security*

United States
Secret Service

Network Architecture

- Refers broadly to overall configuration of network
- Includes type, topology, hardware, speed, and specific cabling used in a given implementation



*U.S. Department of
Homeland Security*

United States
Secret Service

Key Network Architectures

- *Ethernet* – Commonly used network architecture
- *Token Ring* – Obsolete network architecture
- *FDDI* – Often used to connect networks on different floors within a building and where security and performance are a concern
- *Asynchronous Transfer Mode (ATM)* – Often used for large networks in major corporations and government



U.S. Department of
Homeland Security

United States
Secret Service

Ethernet Networks

- Introduced in early 1970s as first shared LAN technology
- Design consists of computers connected to shared transmission medium, such as coaxial cable or multi-port hub
- In general, link computers located in same room or building
- Each host checks cable for turn to transmit data



*U.S. Department of
Homeland Security*

United States
Secret Service

Ethernet Networks

- Uses a bus, star, or tree topology
- Broadcasts data to all devices in network
- Uses CSMA/CD technology to correct data collision on shared network
- Provides good performance for low cost because it is inexpensive to set up
- Installs easily and supports all common protocols
- Work well for small LANs, but problems arise as network grows



*U.S. Department of
Homeland Security*

United States
Secret Service

Ethernet Cabling 10 Base X

- 10 base T – Cat 3 UTP
- 10 base 2 – Thinnet coaxial
- 10 base 5 – Thicknet coaxial
- 10 base FL – Fiber optic



*U.S. Department of
Homeland Security*

United States
Secret Service

Fast Ethernet 100 Base X

- Fast Ethernet offers same shared network protocols as regular Ethernet but with peak transfer rate of 100 Mbps
- Three types of cable used are as follows:
 - 100 base-T4 – Cat 3 UTP cable
 - 100 base-TX – Cat 5 UTP cable
 - 100 base-FX – Fiber optic cable



*U.S. Department of
Homeland Security*

United States
Secret Service

Gigabit Ethernet 1000 Base X

- Gigabit Ethernet offers same shared network protocols as regular Ethernet but with peak transfer rate of 1Gbps
- Speed is achievable on Cat 5e or Cat 6 cable
- All four-wire pairs used instead of just two pairs
- Cable usage provides bi-directional transmissions and receptions



*U.S. Department of
Homeland Security*

United States
Secret Service

Gigabit Ethernet 1000 Base X

- 1000 base-T – Cat 5e or Cat 6 UTP cable
- 1000 base-TX – Cat 6 UTP cable
- 1000 base-CX – Copper cable
- 1000 base-LH – Fiber optic cable
- 1000 base-LX – Fiber optic cable
- 1000 base-ZX – Fiber optic cable



*U.S. Department of
Homeland Security*

United States
Secret Service

Token Ring Network

- All devices linked together in closed loop or ring
- Data packages transmitted via token that travels in one direction around ring
- Token polls each host checking for transmission as it moves around ring
- Hosts must wait for empty token to transmit data
- No other computer can transmit data while token is in use



*U.S. Department of
Homeland Security*

United States
Secret Service

Token Ring Network

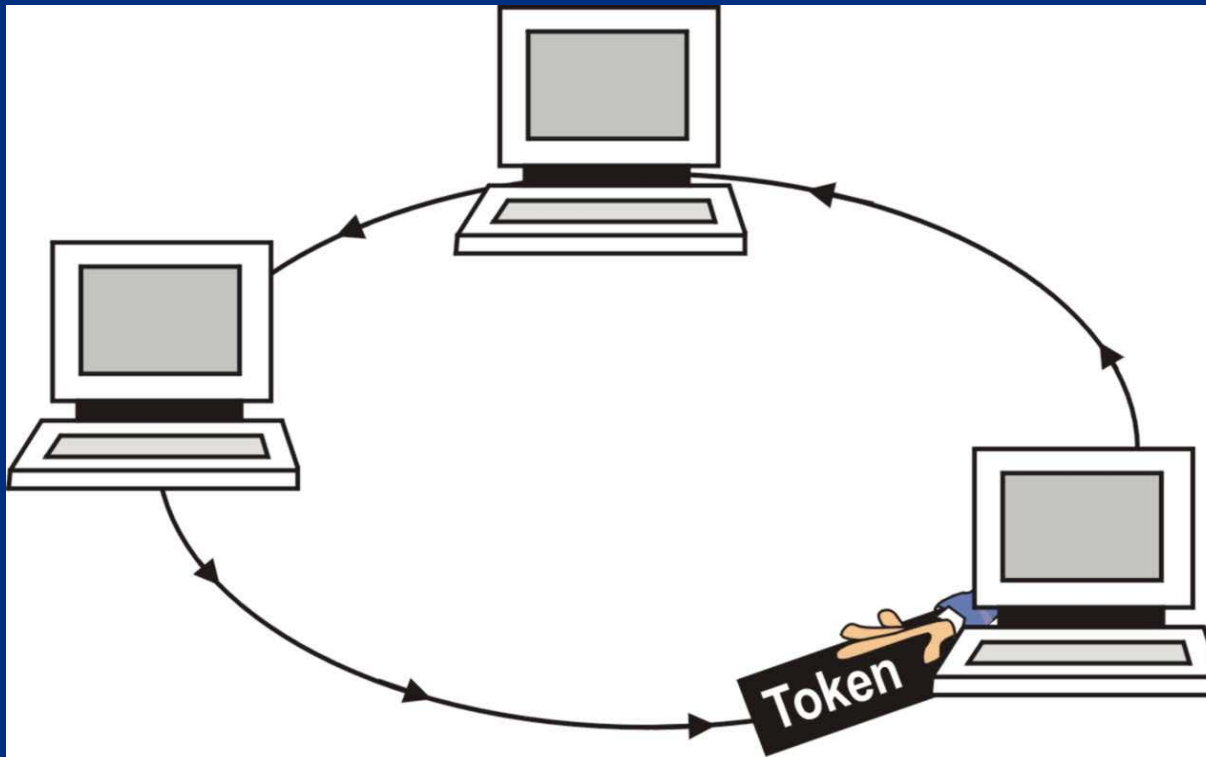
- Normally configured using device called Multistation Access Unit (MAU) to connect computers
- MAU contains logical ring that recognizes attached computers and determines transmission route to them
- Uses ring or star-wired ring topology
- Provides point-to-point communication
- Offers peak transfer rate of 16 Mbps



*U.S. Department of
Homeland Security*

United States
Secret Service

Token Ring Network



*U.S. Department of
Homeland Security*

United States
Secret Service

FDDI Network

- Fiber Distributed Data Interface (FDDI) network uses fiber optic cable to link computers in ring topology
- Data passed using tokens
- FDDI network provides two token rings:
 - Main ring used for all transmissions
 - Second ring only used for backup if main ring fails
- Tokens travel simultaneously in opposite directions



*U.S. Department of
Homeland Security*

United States
Secret Service

FDDI Network

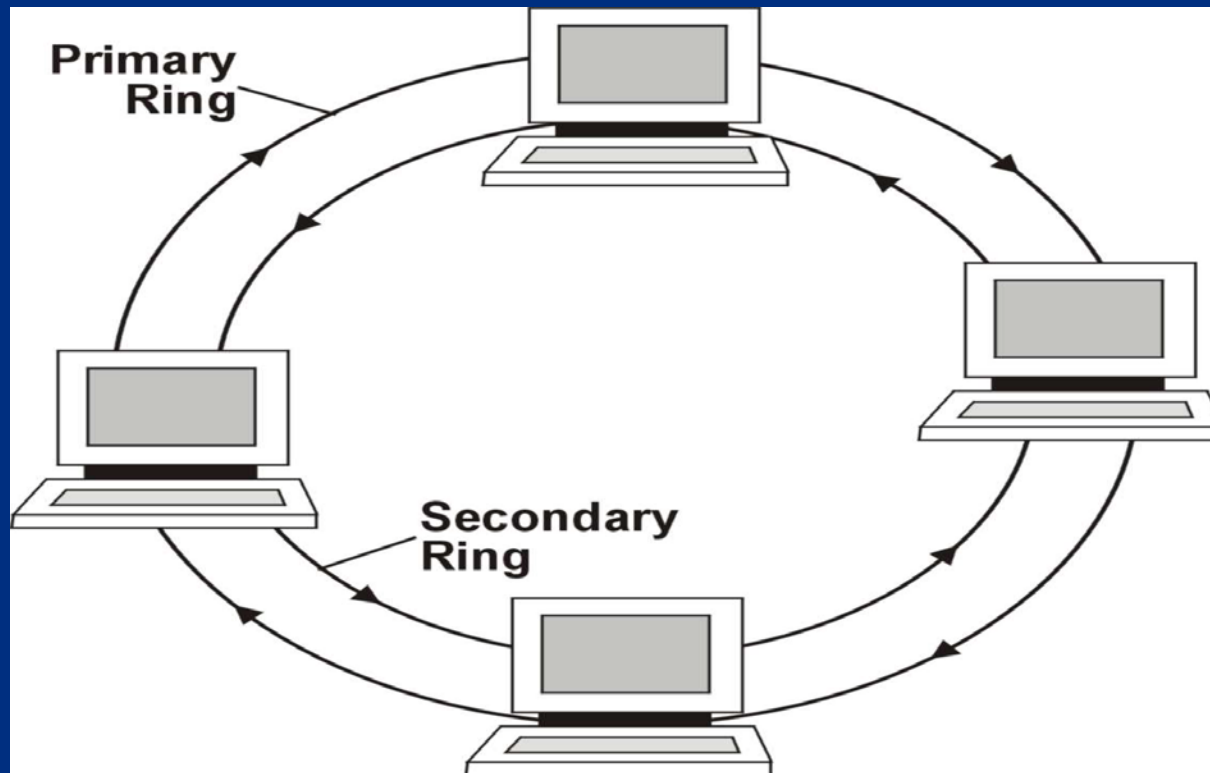
- FDDI uses device called concentrator in lieu of MAU
- Most concentrators can connect between 4 and 32 device
- Fiber optic cable provides higher speeds
- Peak data transfer rate of each ring is 100Mbps (200Mbps for both rings)
- High reliability of FDDI makes it ideal network backbone to support high-end servers



*U.S. Department of
Homeland Security*

United States
Secret Service

FDDI Network



*U.S. Department of
Homeland Security*

United States
Secret Service

ATM Network

- The Asynchronous Transfer Mode (ATM) network performs at high speeds with peak transfer rate of 622 Mbps
- Designed for LANs, WANs, and Internet core networks
- Provides connection-oriented technology that creates circuit between data source and destination
- Divides data into small fixed length cells prior to transmission



*U.S. Department of
Homeland Security*

United States
Secret Service

ATM Network

- Fixed length cells provides high performance and reliability
- Fixed length cells enable predictable traffic flow
- Reliable delivery of time-sensitive data such as live voice and video
- Capable of transmitting different types of traffic simultaneously (isochronous), including data, voice and audio



*U.S. Department of
Homeland Security*

United States
Secret Service

Baseband vs. Broadband

- Data signals sent across transmission media in one of two ways: baseband or broadband
- With baseband, signals are sent down cable in state of “on,” “off,” or “idle”
- Simple transceivers receive signals and translate them into digital 1s and 0s



*U.S. Department of
Homeland Security*

United States
Secret Service

Baseband vs. Broadband

- Broadband more complex in that several streams or channels are sent simultaneously
- With broadband, three states are distinguished by complex transceivers for multiple channels at same time
- In general, baseband is technology used in Ethernet and Token Ring networks
- Broadband used for high speed Internet access



*U.S. Department of
Homeland Security*

United States
Secret Service

Cable Modems

- Cable is broadband technology based on speed, ease of installation, and low cost
- Cable Internet data shared over cable television lines using high frequencies to transmit data and low frequencies for audio and video
- Major drawback, consumers in single network segment share bandwidth
- Segment could be street, neighborhood, or entire community
- More persons connected, lower overall speed for everyone



*U.S. Department of
Homeland Security*

United States
Secret Service

Cable Modems

- Digital cable implements ATM architecture
- Current speeds are between 1 through 6 Mbps
- Future anticipated speed 160 Mbps



*U.S. Department of
Homeland Security*

United States
Secret Service

Digital Subscriber Line Modems

- Digital Subscriber Line (DSL) popular choice for broadband Internet
- Transmits data over telephone lines using higher frequencies than used by voice signals
- Unlike cable Internet, DSL does not share connection speed with others in area
- Speeds usually stay constant throughout day



*U.S. Department of
Homeland Security*

United States
Secret Service

Digital Subscriber Line Modems

- DSL implements ATM architecture
- Current speeds between 256KB and 3 Mbps
- Major drawback, requires consumers to be within 18,000 feet of telephone company's switching station



*U.S. Department of
Homeland Security*

United States
Secret Service

Fiber Optic Service (FIOS)

- Provides fastest data transfer method by sending pulses of light over fiber optic cable
- Fiber cable expensive and service areas difficult to find
- Verizon offers Fiber Optic Service (FIOS) that transmits light signal over fiber optic cable to customer
- When signal reaches customer, Optical Network Terminal (ONT) converts signal from optical to Ethernet
- Connection made to router which in turn connects to customer's computer



*U.S. Department of
Homeland Security*

United States
Secret Service

Fiber Optic Service (FIOS)

- FIOS reaches speeds of 5, 15 or 30 Mbps for downloads
- Speeds of 2 or 5 Mbps for uploads



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 5 – The OSI Model

- OSI Model Overview
- OSI Model Layers



*U.S. Department of
Homeland Security*

United States
Secret Service

OSI Model

- Before OSI model, networks developed and managed as proprietary systems
- Different networks could not communicate with each other
- International Organization for Standardization (ISO) developed OSI model as guideline for protocols to support open networking and communication between multi-vendor systems



*U.S. Department of
Homeland Security*

United States
Secret Service

OSI Model

- Communication sent across network is processed through seven layers of OSI model
- Simply put, OSI model helps data from application, such as a spreadsheet, make its way through network cabling (or other medium) to application on receiving workstation
- OSI model layers represent sequence of procedures



*U.S. Department of
Homeland Security*

United States
Secret Service

Sequence of Procedures Addressed

- Data from transmitting computer is encoded for transmission
- Data is translated into signals and sent
- Data reaches receiving computer
- Data is decoded and displayed on computer



*U.S. Department of
Homeland Security*

United States
Secret Service

Layered Concept

- OSI layers sequentially arranged, each one performs specific tasks
- Data passes from one layer to next after tasks are completed
- Communication from transmitting computer travels down stack from layer seven to layer one before being physically transmitted to receiving computer



*U.S. Department of
Homeland Security*

United States
Secret Service

How Data is Processed

- Network traffic in simplest form is either *request* for information or *reply* that answers request
- All data transmitted over network is divided into packets
- Packets can be of different sizes depending on type of request or reply
- Every request or reply consists of one or more packets



U.S. Department of
Homeland Security

United States
Secret Service

OSI Packet Processing Example

- When transmitting computer makes request, request is divided into one or more packets
- Packet(s) begins journey through sequence of OSI layers
- Network tracks request by adding data to each packet in form of frames
- *Frames* comprised of network control information to ensure packets reach destination in proper form
- Frames generated at various OSI layers



U.S. Department of
Homeland Security

United States
Secret Service

OSI Packet Processing Example

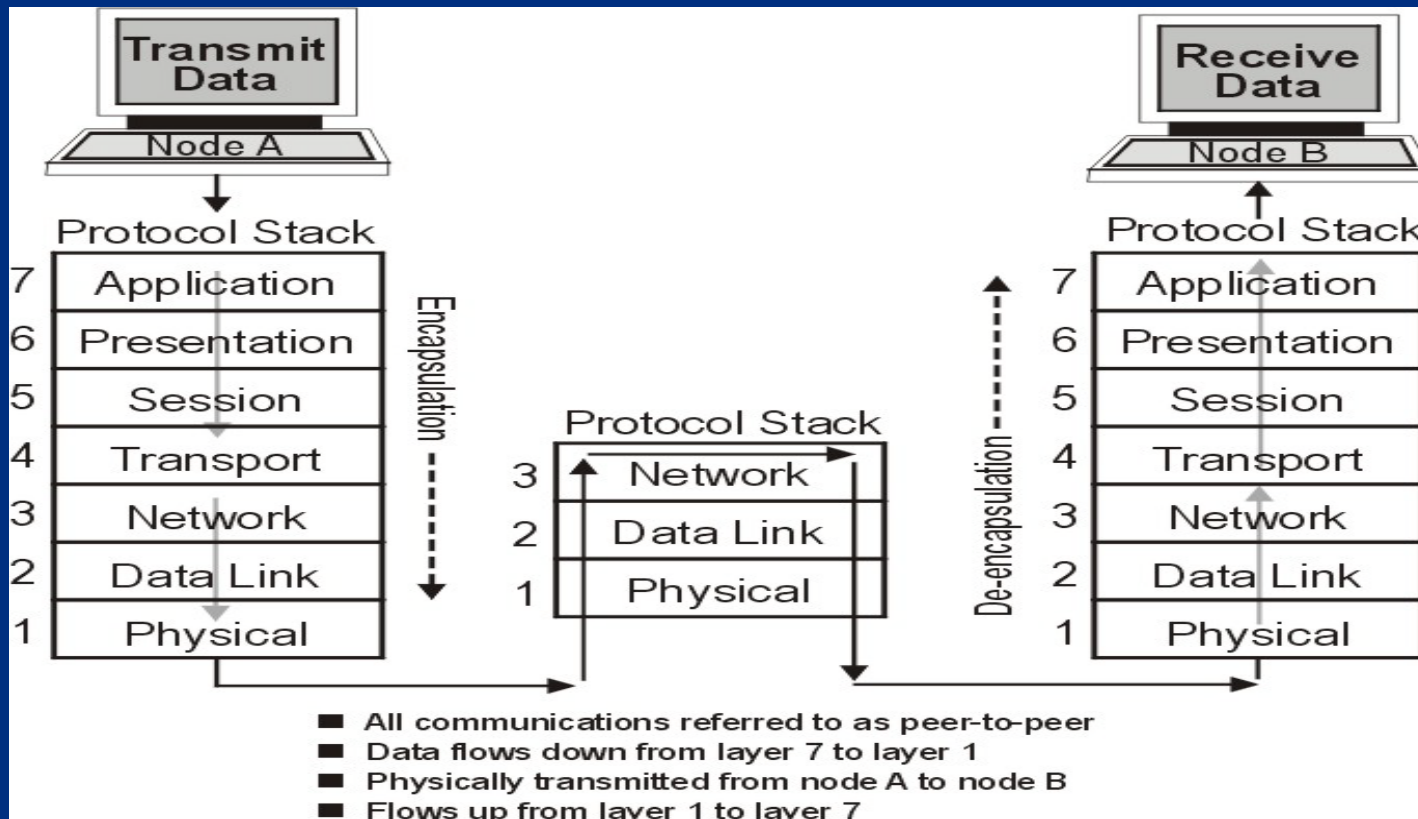
- Packet travels down transmitting protocol stack from layer 7 to layer 1
- Physically transmitted to recipient protocol stack
- Travels up protocol stack from layer 1 to layer 7



*U.S. Department of
Homeland Security*

United States
Secret Service

OSI Protocol Model



U.S. Department of
Homeland Security

United States
Secret Service

OSI Layers

- To conduct computer forensics investigations you must understand how data moves through network
- The seven layers of OSI model describe how data is transported
- Layers divided into two groups: media layers and host layers



*U.S. Department of
Homeland Security*

United States
Secret Service

Media Layers

- Manage physical delivery of data over network
- Physical
- Data link
- Network



*U.S. Department of
Homeland Security*

United States
Secret Service

Host Layers

- Ensure accurate data delivery between PCs
- Transport
- Session
- Presentation
- Application



*U.S. Department of
Homeland Security*

United States
Secret Service

Application Layer (Layer 7)

- Defines interaction between application program and network
- Layer closest to user, interface between application and network
- Example, user working with word processing application requests file stored on network
- Application layer first to process request
- Determines if sufficient resources available to handle request, synchronizes other applications, establishes procedures for error recovery and data integrity



*U.S. Department of
Homeland Security*

United States
Secret Service

Presentation Layer (Layer 6)

- Presentation layer ensures data sent by one application can be interpreted by application on receiving computer
- Sole function is translation of different types of system syntax
- Interprets any formatting codes such as tabs or special characters and formats data for display or printing
- Also performs data encryption and decryption



*U.S. Department of
Homeland Security*

United States
Secret Service

Session Layer (Layer 5)

- Session layer coordinates exchange of data by establishing and managing dialog sessions between end systems
- Sets up connection for data exchange
- Terminates connection when transmission complete



*U.S. Department of
Homeland Security*

United States
Secret Service

Transport Layer (Layer 4)

- Transport layer ensures reliable transmission of data between end systems
- Transfers data at specified level of quality, speed, and error acceptance rates
- Corrects, re-sequences, and reassembles data packets



*U.S. Department of
Homeland Security*

United States
Secret Service

Network Layer (Layer 3)

- Network layer handles complex internetwork routing services to transfer data between two distant networks
- Determines connectivity by first identifying both source and destination address
- Detects errors and resends bad packets
- Translates from hardware to network addresses
- Supports multiple data link connections
- Routes data to alleviate congestion



*U.S. Department of
Homeland Security*

United States
Secret Service

Data Link Layer (Layer 2)

- Data link defines rules for transmitting information across physical connection between two systems
- Concerned with physical addressing as opposed to network or logical addressing
- Provides reliable transit of data
- Creates, receives, and transmits packet frames
- Handles physical device addressing
- Checks for errors



*U.S. Department of
Homeland Security*

United States
Secret Service

MAC Addresses

- Unique physical address that identifies computer for network data transmissions
- Stored on NIC, accessed at data link layer
- When computer on Ethernet network wants to send data packet, uses receiving computer's MAC address to determine pathway
- Data packet carries MAC address of destination computer



*U.S. Department of
Homeland Security*

United States
Secret Service

Physical Layer (Layer 1)

- Physical layer transforms data into binary code so it can be transmitted as electrical or optical signals over cable network
- Defines physical interface between transmission media and network hardware
- Manages all aspects of connection including mechanical components and connectors, electrical aspects such as voltage levels, functional aspects of establishing, maintaining, and ending physical link



*U.S. Department of
Homeland Security*

United States
Secret Service

OSI Layers

- See student book for detailed table defining layers and associated services and devices that operate at each layer



*U.S. Department of
Homeland Security*

United States
Secret Service



*U.S. Department of
Homeland Security*

United States
Secret Service

Mod 6 – Network Connectivity and Protocols



*U.S. Department of
Homeland Security*

United States
Secret Service

You Will Learn . . .

- Network Connectivity
- Network Configuration Models
- Network Protocols
- Wireless Networks



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 1 – Network Connectivity

- Network Connectivity



*U.S. Department of
Homeland Security*

United States
Secret Service

Network Connectivity

- A network connects stand-alone computers, workstations, printers, and other shared resources
- Uses many different types of connection devices



*U.S. Department of
Homeland Security*

United States
Secret Service

Basic LAN components

- Network interface cards (NIC) for each computer
- Transmission media including cabling and connectors



*U.S. Department of
Homeland Security*

United States
Secret Service

Components for Internet Connection

- Modem connected to an Internet Service Provider's modem
- NIC connected to a DSL or cable modem
- USB cable modem
- NIC connected to Optical Network Terminal (ONT)
- Phone wire or UTP cabling as appropriate



*U.S. Department of
Homeland Security*

United States
Secret Service

Network Connection Devices

- Routers to provide transmission pathways between networks
- Hubs to establish central connection point for several network devices on same network
- Repeaters to ensure integrity of signals over long distances
- Switches to direct traffic through network more efficiently
- Multi access units/multi-station access units (MAUs/MSAUs) to set up token ring in star-wired ring topology
- Bridges to connect two separate segments of network



*U.S. Department of
Homeland Security*

United States
Secret Service

Network Transmission Media

- Cable communication:
 - Electric currents or light pulses (for fiber optics) through different types of cabling
- Wireless connections:
 - Radio waves
 - Microwaves
 - light spectrum energy



*U.S. Department of
Homeland Security*

United States
Secret Service

Bandwidth

- Capacity of transmission media, amount of data communication channel can handle
- Bandwidth denoted differently for analog transmissions (phone, radio, and television communications) and digital transmissions
- Analog transmissions measured in cycles per second called hertz (Hz)
- Digital transmissions measured bits per second (bps) and capacity called data transfer rate



*U.S. Department of
Homeland Security*

United States
Secret Service

Three Main Types of Cabling

- Twisted-pair
- Coaxial
- Fiber optic



*U.S. Department of
Homeland Security*

United States
Secret Service

Attenuation

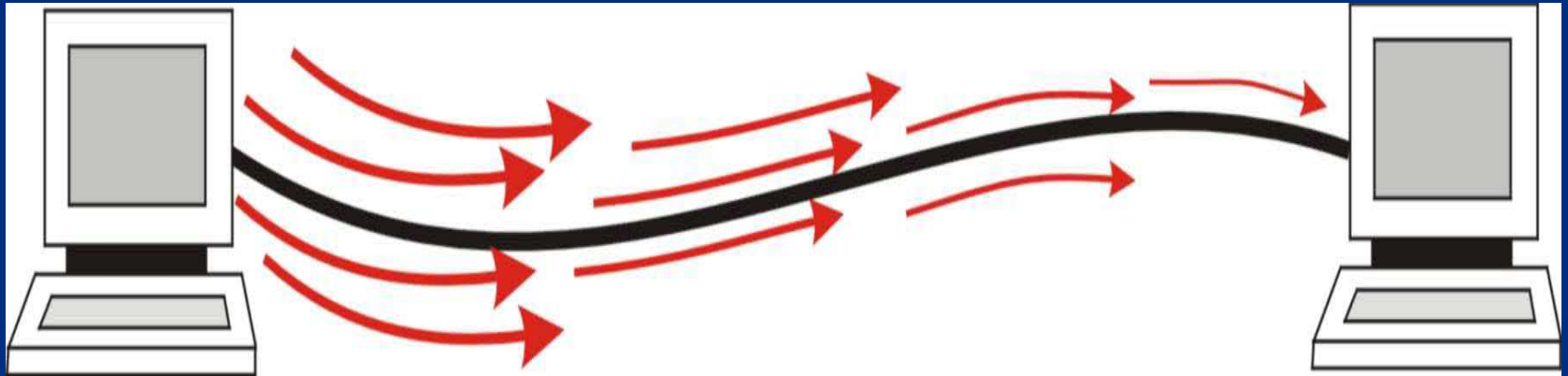
- Signals carried over cabling susceptible to attenuation
- Weakening of signals as they travel away from source
- Specific distance limits for use of cables
- Signals travel limited distance before becoming indecipherable



*U.S. Department of
Homeland Security*

United States
Secret Service

Attenuation



*U.S. Department of
Homeland Security*

United States
Secret Service

Twisted-pair Cabling

- Inexpensive, used extensively with LANs and telephone connections
- Cable consists of individually insulated metal wires twisted together and placed in plastic encasement
- Wires are twisted to prevent crosstalk, noise interference from other wires within same cable
- Twists help prevent electromagnetic interference, or EMI, from nearby electrical or magnetic fields



*U.S. Department of
Homeland Security*

United States
Secret Service

Two Types of Twisted-pair Cabling

- Unshielded twisted-pair (UTP)
- Shielded twisted-pair (STP)
- Shielded cable has additional internal shield covering wires that protects against electromagnetic interference (EMI)
- Electromagnetic waves can be intercepted for eavesdropping on signals
- Neither STP nor UTP offer distance or more reliable interference protection of coaxial or fiber optics



*U.S. Department of
Homeland Security*

United States
Secret Service

Categories of Twisted-pair Cable

- Cat 3 twisted-pair cable supports speeds up to 10 Mbps, commonly used in 10baseT Ethernet networks
- Cat 5 twisted-pair cable supports speeds up to 100 Mbps commonly used in 100baseX Fast Ethernet networks
- Cat 5e twisted-pair cable supports speeds up to 1 Gbps, commonly used in 1000baseX Gigabit Ethernet networks
- Cat 6 twisted-pair cable supports speeds up to 1 Gbps, commonly used in 1000baseX Gigabit Ethernet networks



*U.S. Department of
Homeland Security*

United States
Secret Service

RJ-45 Connectors

- RJ-45 connector used on ends of twisted pair cabling to connect components in Ethernet network
- Has eight-wire modular plug similar in appearance to RJ-11 and RJ-12 (standard phone wire) connectors



*U.S. Department of
Homeland Security*

United States
Secret Service

Coaxial Cable

- Offers greater protection against EMI than twist-pair cabling
- Design has copper core surrounded by insulation and braided metal shield
- Plastic or rubber encasement comprises outside layer
- Widely used for cable television and computer



*U.S. Department of
Homeland Security*

United States
Secret Service

Network Coaxial Cable

- Thinnet coaxial cable
 - Used with 10base2 Ethernet
- Thicknet coaxial cable
 - Used with 10base5 Ethernet



*U.S. Department of
Homeland Security*

United States
Secret Service

Other Coaxial Cable Characteristics

- To build token ring network or bus Ethernet, thinnet used to connect device using T-connector
- Cable must be grounded and terminated
- Peak transfer rate 16 Mbps
- Effective range approximately 185 meters for thinnet and 500 meters for thicknet
- Suffers from high attenuation



*U.S. Department of
Homeland Security*

United States
Secret Service

BNC Connectors

- Acronym for British Naval Connector, Bayonet Neill Canceilman, or Bayonet Nut Connector
- Used to secure Thinnet coaxial cable, found in 10Base2 Ethernet systems
- Has male-type plug found at each end of cable
- Has center pin connected to center cable conductor and metal sheath connected to exterior cable shield
- Rotating ring used to secure connection
- Come in T-connectors, barrel connectors, and terminators



*U.S. Department of
Homeland Security*

United States
Secret Service

Fiber Optic Cable

- Uses glass or plastic fibers to transmit data modulated onto light waves
- Each cable contains two strands in separate jackets
- Fibers can be single-mode allowing only one transmitted signal, or multi-mode allowing multiple transmitted signals simultaneously
- Diameter of optic core of multi-mode fiber visibly larger than single mode fiber



*U.S. Department of
Homeland Security*

United States
Secret Service

Fiber Optic Cable

- Major difference between single-mode and multi-mode fiber is distance they carry signal
- Single-mode fiber, driven by laser light, can carry signal approximately forty-three miles without regeneration
- Multi-mode fiber limited to approximately one and a half miles



*U.S. Department of
Homeland Security*

United States
Secret Service

Fiber Optic Cable

- Data not converted to analog before transmission
- Sent in its original digital format
- Fiber optic offer greater bandwidth
- Can carry more data than metal cables
- Less susceptible to signal interference
- Popular choice for LANs or transoceanic cabling



*U.S. Department of
Homeland Security*

United States
Secret Service

Fiber Optic Cable

- Much thinner and lighter than wire cables
- More fragile to handle and more difficult to cut
- Expensive to install
- Phone companies replacing old lines with fiber optic cables
- May be first choice for future communication cabling



*U.S. Department of
Homeland Security*

United States
Secret Service

Fiber Optic Connectors

- Several different types of connectors depending on application
- End of fiber extends past the connector, damaged easily, should be capped when not in use



*U.S. Department of
Homeland Security*

United States
Secret Service

Network Interface Card (NIC)

- Adapter that enables computer to connect to network
- Each made for network type it will support, such as Ethernet, Token Ring, FDDI
- Some formatted as separate plug-ins to MB while others are integrated into MB
- Most cards work with specific cable types



*U.S. Department of
Homeland Security*

United States
Secret Service

MAC Address

- NICs manufactured with hardwired code unique to each card
- Code called *MAC address*
- First six hexadecimal characters of address represent manufacturer of card
- Last six characters represent serial number of individual card
- Address is essentially computer's physical address on network
- Identifies destination for transmitting data packets on network



U.S. Department of
Homeland Security

United States
Secret Service

More About NICs

- Laptop and notebook computers can have NIC built into MB or use NIC in form of PC card
- Slot on side of laptop holds PC card and provides high-speed access to processor and memory
- Several NICs for both Ethernet and Token Ring
- NICs used for FDDI called Dual Access Stations (DAS) as they connect computer to each of two separate token rings



*U.S. Department of
Homeland Security*

United States
Secret Service

How NICs Work

- When computer makes request to communicate with network OS sends request to NIC
- NIC converts request into proper type of data packets
- Monitors network traffic flow and sends packets at appropriate time when there is opening
- Checks MAC addresses of passing network transmissions
- If addressed to computer, NIC copies packet for computer
- NICs work at Data Link Layer 2 of OSI Model



*U.S. Department of
Homeland Security*

United States
Secret Service

Modems

- Handle communications transmitted over telephone lines between computer systems
- Most have fax capabilities
- Converts or modulates PC's digital code to analog so it can be sent over phone cables
- Converts or demodulates analog signals to digital code before transmitting data to PC
- Modems work at Physical Layer 1 of OSI Model



*U.S. Department of
Homeland Security*

United States
Secret Service

Asynchronous Transmission Mode

- Sends data intermittently one character at a time
- A start bit and stop bit frame each character



*U.S. Department of
Homeland Security*

United States
Secret Service

Synchronous Transmission Mode

- Relies on software to negotiate protocol used
- Blocks of data much larger (128 up to 1024 bytes or more) than with asynchronous mode communications
- Receiving modem must respond with acknowledgement (ACK) of receipt or negative acknowledgement (NAK)



*U.S. Department of
Homeland Security*

United States
Secret Service

Hubs

- Contains ports to connect network computers and devices
- Provides central point of connection for network nodes
- Type connector needed by each node depends on network architecture and cabling used (i.e., Ethernet, Fast Ethernet, etc)
- Most are small boxes with multiple ports
- Some hubs are cards that can plug into a server



*U.S. Department of
Homeland Security*

United States
Secret Service

Types of Hubs

- Passive Broadcast Hub:
 - Broadcasts data packets to every node on hub
 - Performs no signal regeneration
- Active Broadcast Hub:
 - Broadcasts data packets to every node on hub
 - Enhances signal transmission by regenerating signals and filtering noise



*U.S. Department of
Homeland Security*

United States
Secret Service

More About Hubs

- Intelligent hub, essentially active hub that contains network management functions used to gather information on network traffic and error detection
- Most intelligent hubs can monitor individual ports and close port if problems arise
- Hubs do not decide when or where to send data packets
- Simply broadcast data to all ports
- Hubs work at Physical Layer 1 of OSI Model



*U.S. Department of
Homeland Security*

United States
Secret Service

Token Ring MAU/MSAU

- Multi-Station Access Unit (MAU/MSAU), device used to link nodes on token ring networks
- Nodes connected to MAU and data packets routed in ring
- Star-wired ring topology makes it easy to add or remove nodes
- Devices decide where to send data packets and create point-to-point connection based on sending and receiving node's MAC addresses
- Work at Data Link Layer 2 of OSI Model



*U.S. Department of
Homeland Security*

United States
Secret Service

Repeater

- Combat attenuation by boosting signal during transmission
- Analog repeaters amplify, digital repeaters regenerate signal
- Can relay signals between networks that use different types of protocols or cabling
- Repeaters do not decide when to send data
- Receive data packets in one port, regenerate or amplify, and send back out other port
- Work at Physical Layer 1 of OSI Model



*U.S. Department of
Homeland Security*

United States
Secret Service

Bridge

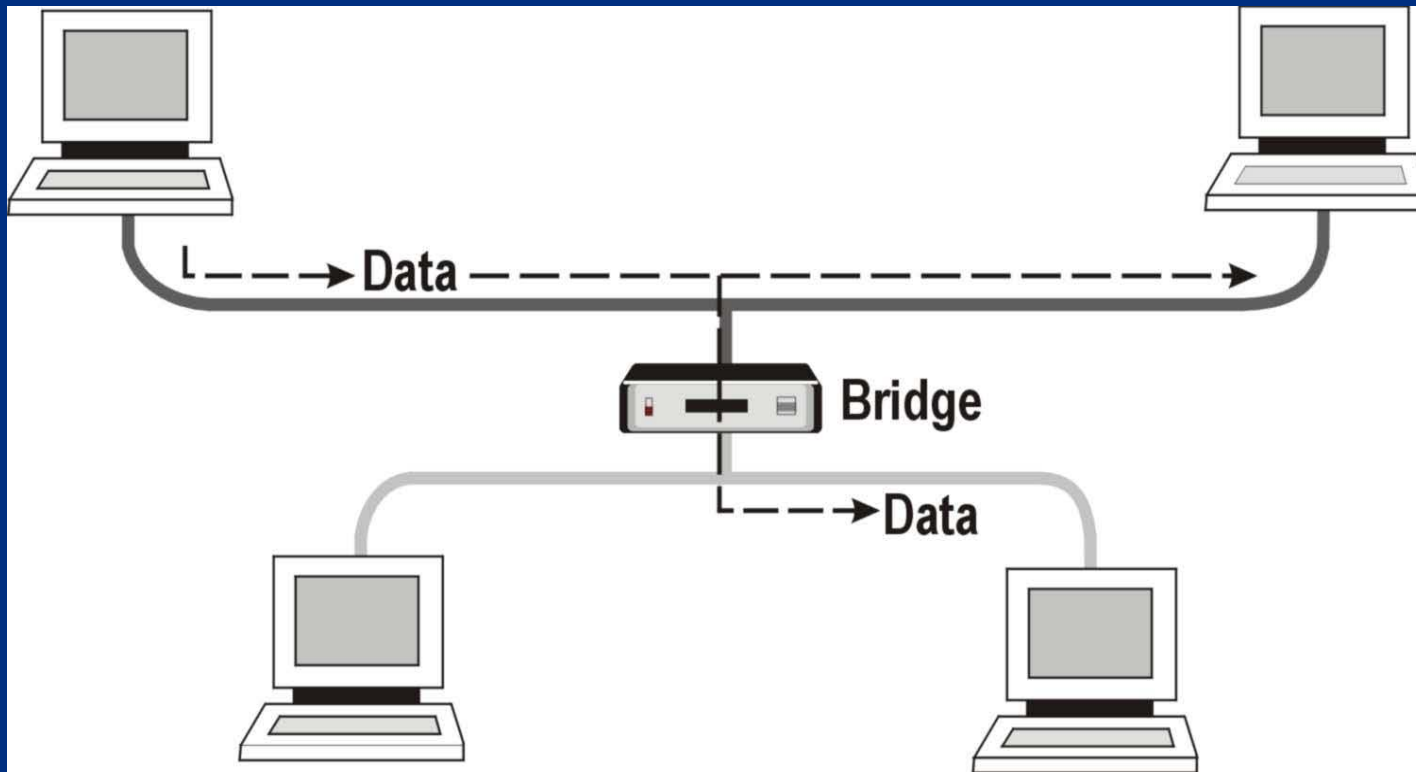
- Joins two separate segments of same network
- Can be used to divide overloaded network by creating separate broadcast (collision) domains
- Can connect two dissimilar networks, such as connecting Ethernet with Token Ring network



*U.S. Department of
Homeland Security*

United States
Secret Service

Bridge Example



*U.S. Department of
Homeland Security*

United States
Secret Service

Bridge

- Decides whether data packets should be sent from one collision domain, across bridge, into second collision domain, based on MAC address of sending and receiving nodes
- If sending and receiving nodes on same segment, bridge simply ignores, or drops packets
- Works at Data Link Layer 2 of OSI Model



*U.S. Department of
Homeland Security*

United States
Secret Service

Switches

- Visibly resemble hubs, help increase speed of network by providing dedicated bandwidth to each port
- Functions like cross between bridge and hub
- Cut down on amount of broadcast traffic on network segment
- Directs network packets from incoming port directly to port for receiving computer
- Lowers number of collisions on network segments, improving overall performance



*U.S. Department of
Homeland Security*

United States
Secret Service

Switches

- Can be managed, allowing individual port configuration and monitoring from across network
- Direct packets based on sender and receiver MAC addresses
- Have ability to broadcast to all ports when necessary, differ from hubs in that they limit traffic to sender and receiver ports without broadcasting
- Work at Data Link Layer 2 of OSI Model
- Also Layer 3 switches, direct data based on network address



*U.S. Department of
Homeland Security*

United States
Secret Service

Routers

- Link separate networks or LAN segments and establish pathways for data packet transmissions
- Use network addresses to transmit packets to correct destination
- Transmit data packets across different types of networks
- Fragment data packets to fit different frame sizes of various networks
- Can be configured to segregate secure data and prevent it from being sent to specified networks



*U.S. Department of
Homeland Security*

United States
Secret Service

Routers

- Collect and assemble information from remote routers about network routes, information used to identify reliable pathways
- Do not broadcast data packets
- Read each data packet looking for network address (IP address) to send to
- Determine best route to forward packets and replace sender's MAC address with its own



*U.S. Department of
Homeland Security*

United States
Secret Service

Routers

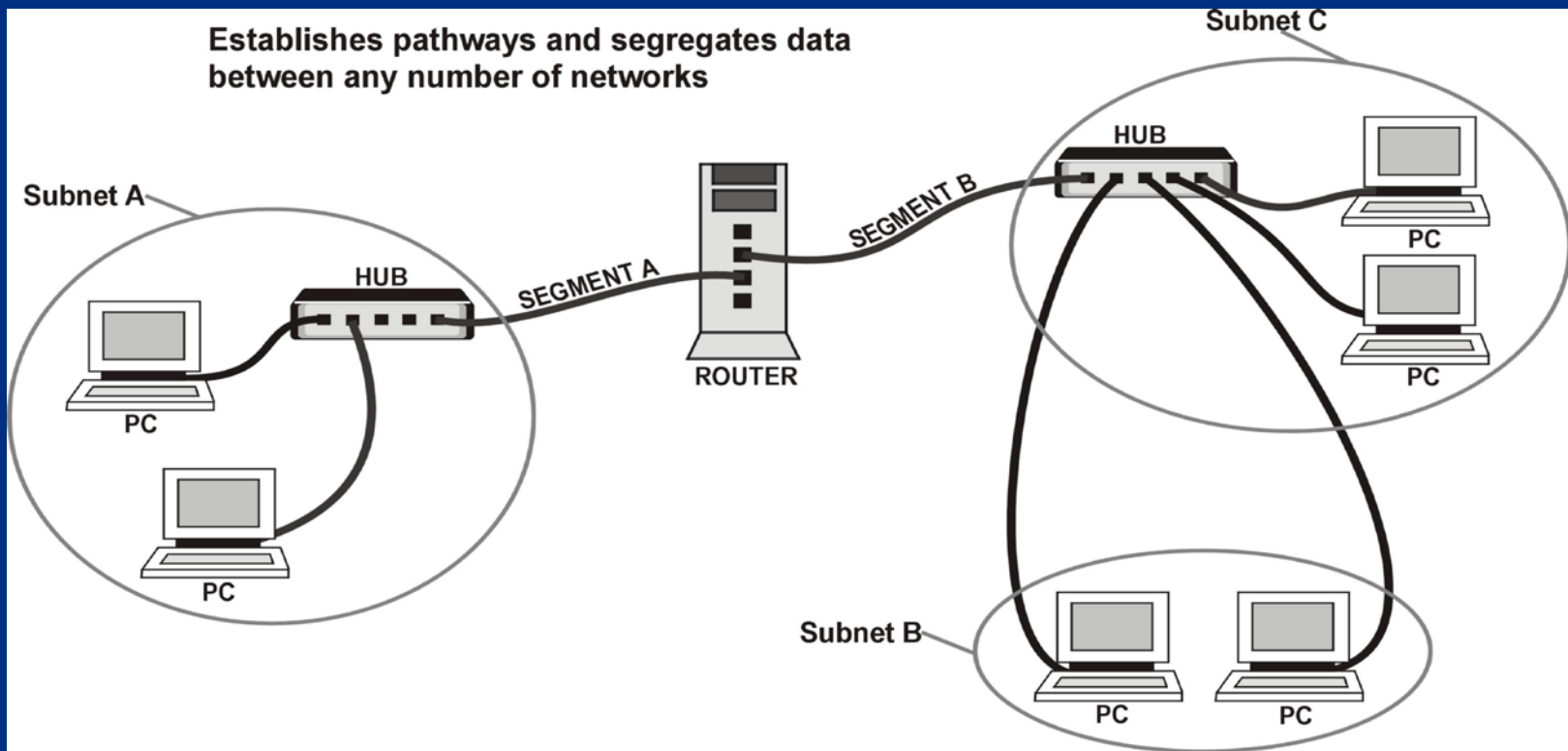
- Each port on router is in essence a separate NIC with its own unique MAC address
- As packets move from one router to another, MAC address in packets change from router to router
- Original source and destination IP addresses remain same regardless of how many routers packet encounters



*U.S. Department of
Homeland Security*

United States
Secret Service

Router Model



*U.S. Department of
Homeland Security*

United States
Secret Service

Routing Activity

- Routers on networks exchange information about paths through process known as *convergence*
- Convergence information stored in routing tables, which contain network portion of host computer's IP address
- Routing assumes addresses convey at least partial information about where host is located
- Permits routers to forward packets without having to rely on complete list of all possible destinations



U.S. Department of
Homeland Security

United States
Secret Service

Two Basic Routing Activities

- Path determination
 - Enables routing protocol to determine best direction to route packet
 - Determination will differ based on routing protocol used
- Switching
 - Involves router forwarding packets independently through network
 - Forwards packets based on IP address, function of Network Layer 3 of OSI Model



*U.S. Department of
Homeland Security*

United States
Secret Service

Gateway

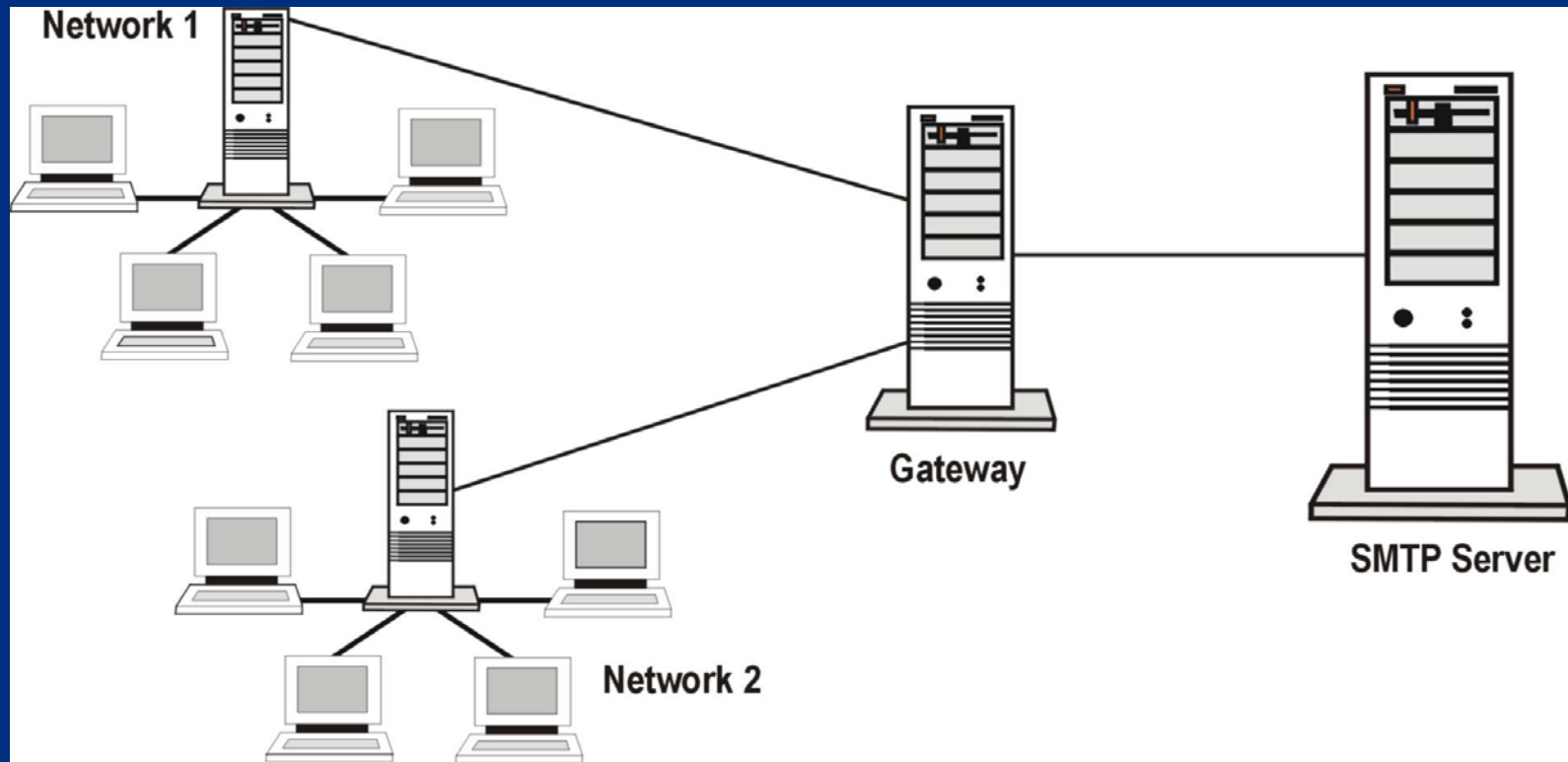
- Server or software program that is entrance point to network
- Can translate different protocols on network
- Can serve as proxy servers and firewalls
- Able to look at data inside packets and perform high-level decisions about data beyond simply looking at MAC or network address
- Functions at Layers 4 - 7 of OSI Model



*U.S. Department of
Homeland Security*

United States
Secret Service

Gateway Example



*U.S. Department of
Homeland Security*

United States
Secret Service

Wireless Media

- Offers data communications between computers without use of traditional network wire or cabling
- Data transmitted over frequencies in air rather than through cable
- IEEE 802.11 standard defines all aspects of radio frequency wireless networking



*U.S. Department of
Homeland Security*

United States
Secret Service

Two Types of Wireless Systems

- Fixed wireless
 - Describes computing devices or networks in fixed locations, such as building, office, or home
 - Devices rely on electrical power
- Mobile wireless
 - Portable computing devices, such as cell phones, PDAs, and wireless notebooks that use battery power and can transmit and receive from any location



*U.S. Department of
Homeland Security*

United States
Secret Service

How Wireless Communications Works

- Wireless Access Points (WAPs), base stations, are devices clients use to connect to wireless networks
- Devices transmit and receive signals without electrical or optical conductors
- Communication uses Earth's atmosphere as physical data path



*U.S. Department of
Homeland Security*

United States
Secret Service

How Wireless Communications Works

- Uses technology in radio frequency (RF) transmissions to send network packets across airwaves
- Typical indoor ranges are 150-300 feet and outdoor ranges up to 1,000 feet
- RF technology used in both LANs and WANs



*U.S. Department of
Homeland Security*

United States
Secret Service

How Wireless Communications Works

- Laptop computers have transceivers in PC-card slots that connect to wireless access point (WAP) and wired network
- Desktop PCs use either ISA/PCI wireless or USB transceiver
- Data transfer speeds can be slower than wired connections



*U.S. Department of
Homeland Security*

United States
Secret Service

Wireless LAN

- Wireless LAN, WLAN, transmits over air, do not require arranging devices for line of sight transmission
- WAPs are connected to Ethernet hub or server
- Send radio frequency signals through walls over area up to 1,000 feet
- Desktop PCs send and receive transmissions via ISA or PCI card
- Laptops use PC cards or wireless modems that connect to Ethernet port



*U.S. Department of
Homeland Security*

United States
Secret Service

Wireless Signals

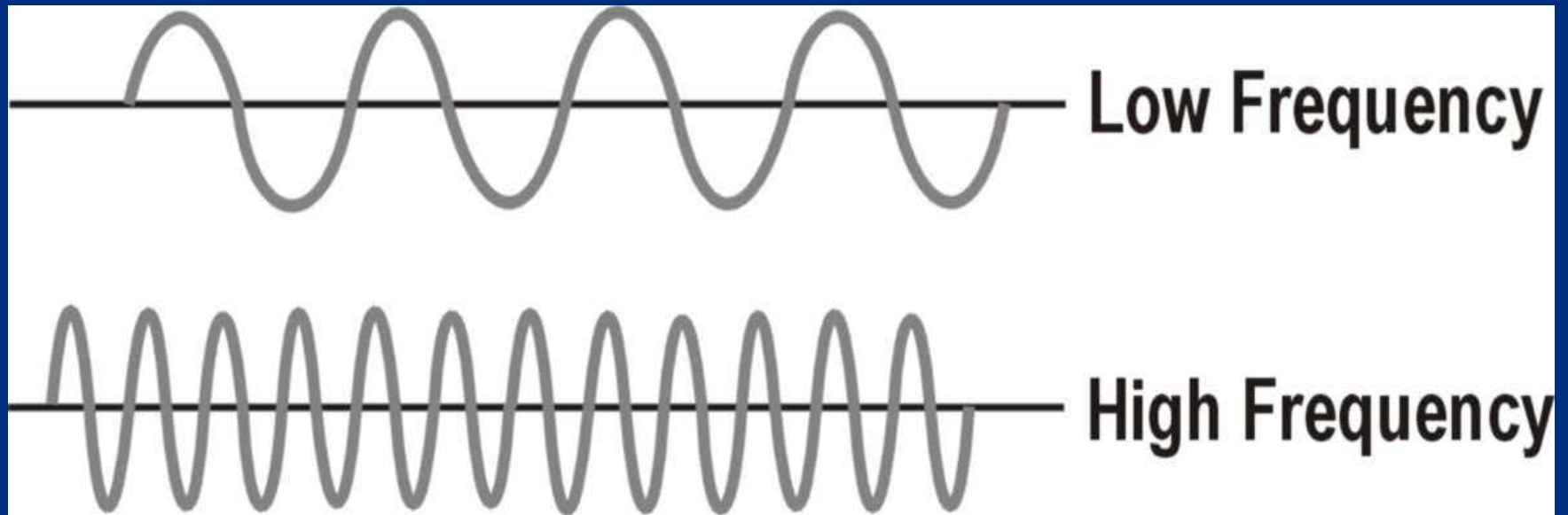
- Wireless signals operate at frequency rate gauged by number of oscillations per time unit signal makes
- Faster the cycle rate, higher the frequency
- High frequency has more oscillations per second than low frequency



*U.S. Department of
Homeland Security*

United States
Secret Service

Frequency Illustration



*U.S. Department of
Homeland Security*

United States
Secret Service

Wireless Signals

- Wireless signal frequencies measured in hertz (Hz)
- Most current wireless communications involve megahertz (MHz) and gigahertz (GHz)
- Higher hertz rates mean greater bandwidth and more data capacity



*U.S. Department of
Homeland Security*

United States
Secret Service

Types of Wireless Signals

- Radio frequency (RF) signals
- Microwaves
- Infrared signals



*U.S. Department of
Homeland Security*

United States
Secret Service

Radio Frequency (RF)

- Majority of wireless communication transmitted over RF
- High Frequency (HF): 3 – 30 MHz
- Very High Frequency (VHF): 30 – 300 MHz
- Ultra High Frequency (UHF): 300 MHz – 3 GHz
- Super High Frequency (SHF): 3 GHz – 30 GHz
- Devices that use RFs between 10KHz and 1GHz include short wave radio, VHF television, FM radio, and UHF radio television



*U.S. Department of
Homeland Security*

United States
Secret Service

Types of RFs

RF	Characteristics
Low Power, Single-Frequency	Used to carry signals short distances. This method is susceptible to massive attenuation and vulnerable to eavesdropping.
High-Power, Single-Frequency	Used over long distances. They can resist attenuation, but are vulnerable to eavesdropping.



*U.S. Department of
Homeland Security*

United States
Secret Service

Types of RFs

RF	Characteristics
Spread Spectrum	<p>Uses multiple frequencies simultaneously and continuously to change signal patterns. Two types of spread spectrum RFs:</p> <ul style="list-style-type: none">• Direct Sequence Modulation: Transmits encoded data and white noise across subnet of radio frequencies. Most common RF used.• Frequency Hopping: Switches between pre-established frequencies several times per second.



*U.S. Department of
Homeland Security*

United States
Secret Service

Microwave Wireless Media

- Microwaves are electromagnetic waves that use same frequencies as RFs
- Two basic forms of microwave communication, both susceptible to weather conditions, jamming frequencies, eavesdropping, and latency
- Terrestrial: Sends data over land such as for line-of-sight transmissions between buildings
- Satellite: Sends data across great distances via satellites



*U.S. Department of
Homeland Security*

United States
Secret Service

Infrared Wireless Media

- Infrared transmissions use optical transceivers to communicate between transmitter and receiver
- Operate using line-of-sight or reflection and require unobstructed pathway between devices



*U.S. Department of
Homeland Security*

United States
Secret Service

Infrared Wireless Media

- Point-to-Point Infrared:
 - Uses tightly focused beams directed at specific receiver (s) such as one computer transmitting to another within same area
- Broadcast Infrared:
 - Signals diffused over wide area to number of receivers such as data sent to several computers within a room
 - Data transfer is slow



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 2 – Network Configuration Models

- Introduction to Network Models



*U.S. Department of
Homeland Security*

United States
Secret Service

Network Models

- Peer-to-peer network
- Client/server network
- Server-centric network, which includes:
 - Enterprise network
 - Server/server network
 - Remote access service (RAS) network



*U.S. Department of
Homeland Security*

United States
Secret Service

Peer-to-Peer Network Model

- Computers linked function as both workstations and servers to share resources
- PC's can share drives, printers, and other common devices while running applications
- Easy to set up and often found in small offices
- Limited user security can be configured to include password access
- Not ideal for large network where server-based network can provide more security



*U.S. Department of
Homeland Security*

United States
Secret Service

Client/Server Network Model

- Individual workstations send requests to central server and server provides resources
- Separation of duties makes for powerful system
- Fast processing time for running applications
- Increased disk space for sharing files
- Network security including mandatory user login to access network resources



*U.S. Department of
Homeland Security*

United States
Secret Service

Client/Server Network Model

- Has advantages over peer-to-peer network
- Provides more organized system, resources easier to locate
- Better security features, all user login files stored in one location
- All users have profile that includes login name and password
- User validation must occur before network access granted



*U.S. Department of
Homeland Security*

United States
Secret Service

Server-centric Network Model

- Each server has defined roles and offers access to specific shared resources
- Each server requires user login authentication before processing requests



*U.S. Department of
Homeland Security*

United States
Secret Service

Enterprise Network Model

- Connects all departmental and individual networks into one network allowing exchange and access of resources across organization
- Integrates all systems types to link in enterprise network
- Interconnectivity achieved with TCP/IP and other Web technologies
- Designated server maintains system security
- Users login once for access across network



*U.S. Department of
Homeland Security*

United States
Secret Service

Server/Server Network Model

- One server provides services to other servers in network
- Types of services provided include domain name service (DNS) address resolution and dynamic host configuration protocol (DHCP) IP address request and issue



*U.S. Department of
Homeland Security*

United States
Secret Service

Remote Access Service (RAS)

- Enables users to access network from any outside location by using modem or Internet connection



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 3 – Network Protocols

- Protocols
- TCP/IP
- Other Protocols



*U.S. Department of
Homeland Security*

United States
Secret Service

Protocols

- Define rules for transmitting data between computers or other devices
- Determine size of data packets, type of information included in each packet, what actions take place if communication does not reach destination



*U.S. Department of
Homeland Security*

United States
Secret Service

Protocol Guidelines

- Provide data compression, when necessary
- Determine process to begin and end a communication
- Govern message routes and data speeds
- Provide error checking procedures to ensure error-free message delivery
- Offer translation services for different types of computers and networks



*U.S. Department of
Homeland Security*

United States
Secret Service

Protocols Covered in This Lesson

- TCP/IP
- IPX/SPX
- NetBEUI/NetBIOS
- PPP/PPTP



*U.S. Department of
Homeland Security*

United States
Secret Service

TCP/IP

- Transmission Control Protocol/Internet Protocol (TCP/IP) considered standard protocol for the Internet
- Can be used for internal networks without Internet access
- Must be used for device to gain Internet access



*U.S. Department of
Homeland Security*

United States
Secret Service

TCP/IP

- Suite of communications protocols governing how data travels between devices and networks throughout Internet
- Developed in 1969 to interconnect networks of research agencies around country
- Designed to work on all network topologies and communicate over fiber optics, twisted-pair, or coaxial cable



*U.S. Department of
Homeland Security*

United States
Secret Service

TCP Functions

- Divide data into manageable packet sizes
- Reassembles data at destination
- Verifies packet arrival at destination
- Transport Layer 4 of OSI Model



*U.S. Department of
Homeland Security*

United States
Secret Service

IP Functions

- Defines how much data can be carried by each packet
- Packages and addresses data to be sent
- Enables various types of networks to read and route data packets
- Network Layer 3 of OSI Model



*U.S. Department of
Homeland Security*

United States
Secret Service

TCP/IP Message Routing

- TCP/IP is routable protocol that enables computers on different networks to communicate as if on same network
- IP part of protocol provides routing capability
- Sent message divided into packets
- TCP/IP determines travel path and transmits packets
- When packet reaches destination, confirmation sent to source
- Confirmation is why TCP/IP is considered to be so reliable



*U.S. Department of
Homeland Security*

United States
Secret Service

TCP/IP Suite Protocols

- Simple Mail Transfer Protocol (SMTP) – Used to send email
- File Transfer Protocol (FTP) – Used to transfer files
- Simple Network Management Protocol (SNMP) – Used to monitor network activities
- Telnet – Allows logon to remote computer to run program
- Domain Name Service (DNS) – Matches domain names of host computers with corresponding IP addresses



*U.S. Department of
Homeland Security*

United States
Secret Service

TCP/IP Model

- Application layer
- Transport layer
- Network layer
- Link layer



*U.S. Department of
Homeland Security*

United States
Secret Service

Encapsulation

- A TCP/IP process for handling data packets
- As data travel down TCP/IP model when a device transmits packets, each layer adds leading information, or headers



*U.S. Department of
Homeland Security*

United States
Secret Service

De-capsulation

- The process of removing headers as data travels up TCP/IP model on receiving network device



*U.S. Department of
Homeland Security*

United States
Secret Service

TCP/IP vs. OSI Model

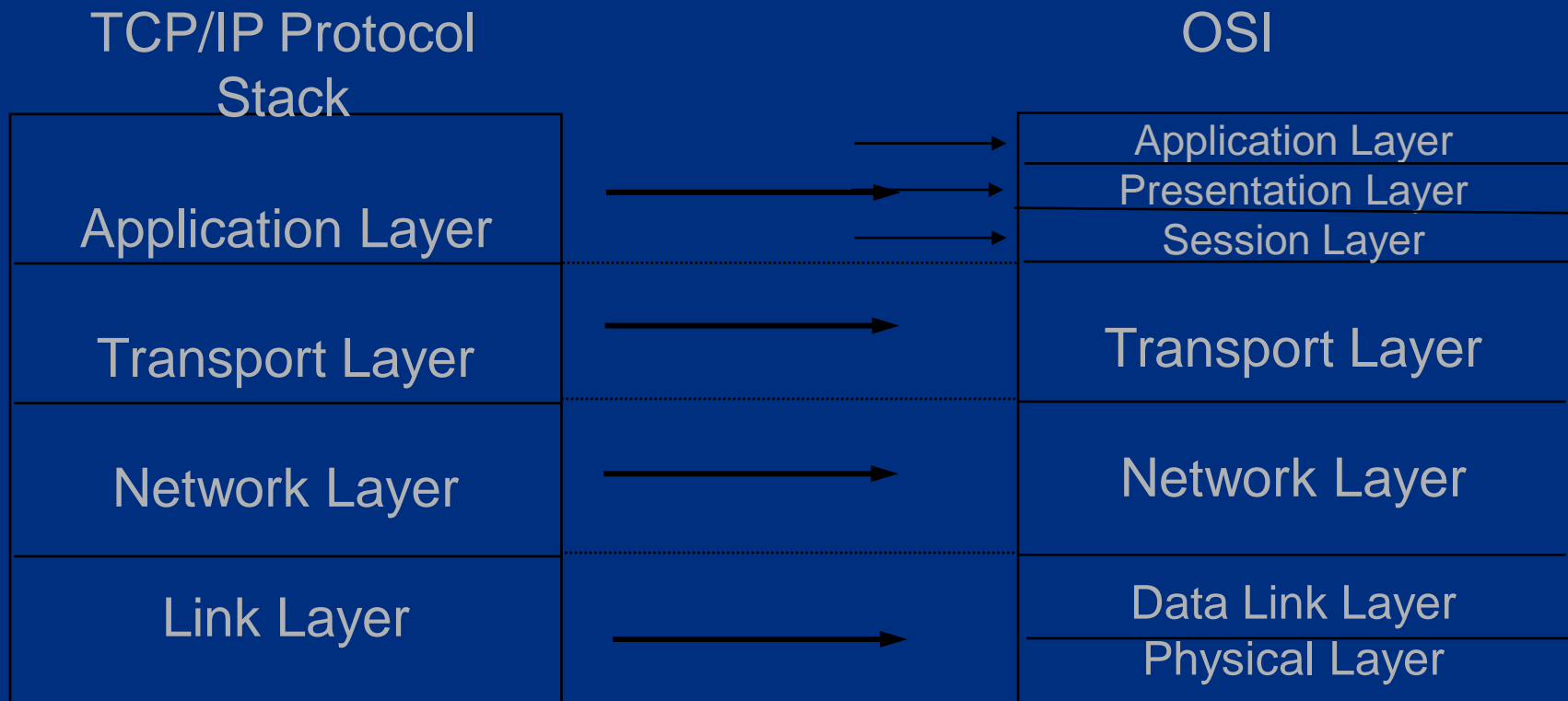
- OSI considered conceptual model of how communications should flow from one network to another
- OSI Provides standard for other protocols to use
- TCP/IP represents actual implementation of how internetwork communications occur
- TCP/IP Application layer absorbs functions of OSI Model's Presentation and Session layers
- TCP/IP combines functions of Data Link and Physical layers of OSI Model



*U.S. Department of
Homeland Security*

United States
Secret Service

TCP/IP vs. OSI Model Illustration



*U.S. Department of
Homeland Security*

United States
Secret Service

Internetwork Packet Exchange (IPX)

- Novell Netware protocol
- Easy to configure for small networks and compatible with other network operating systems
- IPX is connectionless network protocol operates on Network Layer
- IPX data packets sent without prior knowledge of current state of recipient system
- Packet delivery not guaranteed



*U.S. Department of
Homeland Security*

United States
Secret Service

Sequenced Packet Exchange (SPX)

- Novell Netware protocol
- Easy to configure for small networks and compatible with other network operating systems
- Connection-oriented, ensures proper delivery of packets by establishing virtual connection between sender and receiver before packets sent
- Guarantees delivery of packets and provides error correction and packet sequencing



*U.S. Department of
Homeland Security*

United States
Secret Service

NetBIOS

- Standard networking protocol for Windows networks
- Provides programming interface for applications on Session Layer
- Combined with NetBIOS Extended User Interface (NetBEUI), which serves as default transport protocol for Windows networks



*U.S. Department of
Homeland Security*

United States
Secret Service

NetBEUI

- Each computer on NetBEUI network has unique NetBIOS name (no more than 15 characters)
- Non-routable, cannot pass data through router to leave LAN
- Broadcasts many packets which makes it difficult to scale
- Easy to configure with low overhead
- Fast, self-tuning
- Best suited for small LANs



*U.S. Department of
Homeland Security*

United States
Secret Service

Point-to-Point Protocol (PPP)

- Designed for simple links between two peers
- Offers full-duplex operation to both peers
- Packets delivered in order (circuit-switched)
- Used to link PC to Internet
- Creates session between PC and ISP
- Works well with many protocols including IPX



*U.S. Department of
Homeland Security*

United States
Secret Service

Point-to-Point Tunneling Protocol (PPTP)

- Enables other protocols to transmit over IP network
- For example, used to encapsulate NetWare IPX packets and send them over Internet
- Also used to carry TCP/IP, IPX/SPX, and NetBEUI traffic



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 4 – Wireless Networks

- What is a Wireless Network?
- Types of Wireless Networks
- Hardware Components
- Security Concerns
- Vulnerabilities



*U.S. Department of
Homeland Security*

United States
Secret Service

Wireless Network

- Does not require cables to connect computers and peripherals
- Network communications transmitted across airwaves using infrared and various forms of radio technology
- Uses radio frequencies between 2 and 5 gigahertz
- Growing in popularity
- Effective range between 300 and 1,500 feet



*U.S. Department of
Homeland Security*

United States
Secret Service

802.11

- Established global rules for wireless networking at speed of 2Mb/sec
- 802.11b, extension of original standard, increased throughput from to 11Mb/sec
- 802.11b operates at frequency of 2.4 gigahertz, backward compatible with original standard



*U.S. Department of
Homeland Security*

United States
Secret Service

802.11

- Extensions 802.11a and 802.11g, both offer throughput as high as 54Mb/sec
- 802.11g, backward compatible with 802.11b, both operate at 2.4 gigahertz
- 802.11n claims to be twice as fast as 802.11g,
- 802.11i addresses security concerns over current 802.11 standards
- 802.11n incorporates Multiple Input Multiple Output (MIMO) antennas



*U.S. Department of
Homeland Security*

United States
Secret Service

Hot Spots

- 802.11 networking feature often packaged under label *Wi-Fi* and *Centrino*, an Intel trademark
- Intel partnered with companies like Hilton Hotels & Resorts, Borders Group, and McDonalds to develop concept called *hot spots*
- Enables user of wireless-enabled notebooks and PDAs to connect to Internet while using other services business offers
- Strategy is two-fold: wireless hardware sales increase, and hosting businesses attract more customers



U.S. Department of
Homeland Security

United States
Secret Service

Types of Wireless Networks

- In general, two types of wireless networks: ad-hoc and infrastructure
- Type of network simply indicates how wireless devices are configured to communicate
- Configuration can be easily changed from one type to other making wireless networking flexible and easy to use



*U.S. Department of
Homeland Security*

United States
Secret Service

Ad-Hoc Wireless Network

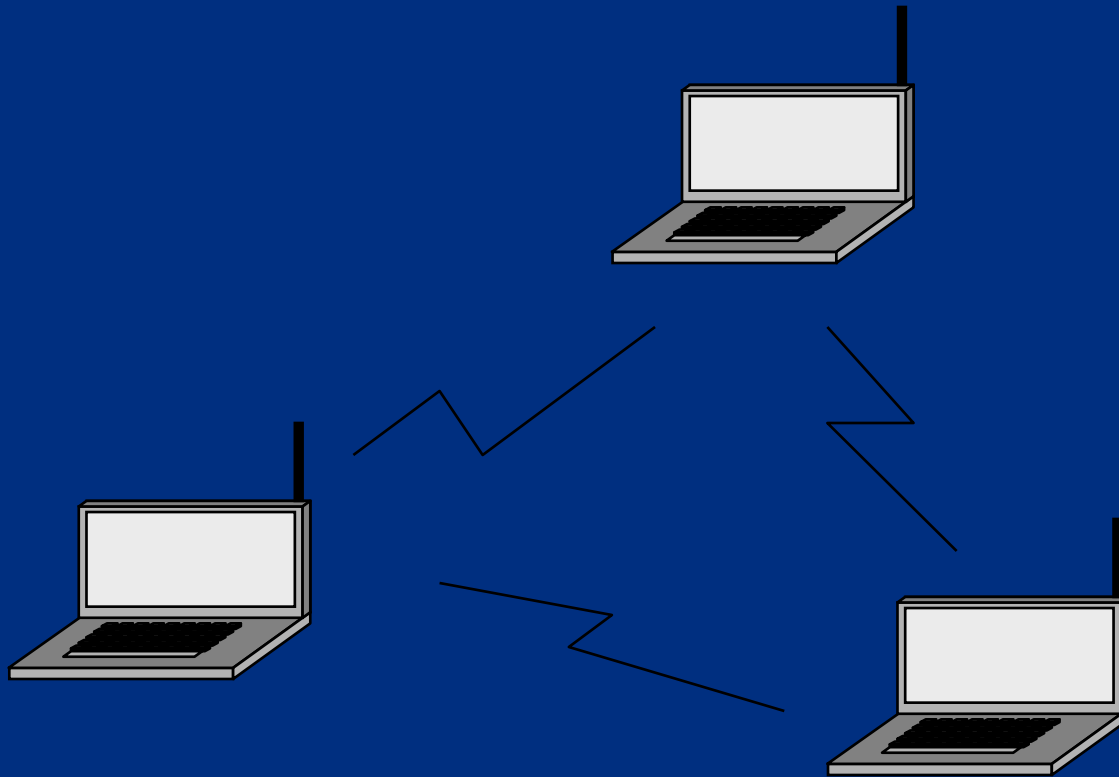
- When group of wireless computers configured to communicate with each other in peer-to-peer configuration, result is independent wireless network
- Combination of wireless computers and modern operating systems allow enough flexibility for wireless computers to join network with ease
- Provides easy setup, ideal for groups who wish to collaborate on project
- Ad-hoc nature of network provides wireless network its name



*U.S. Department of
Homeland Security*

United States
Secret Service

Ad-Hoc Wireless Network



*U.S. Department of
Homeland Security*

United States
Secret Service

Infrastructure Wireless Network

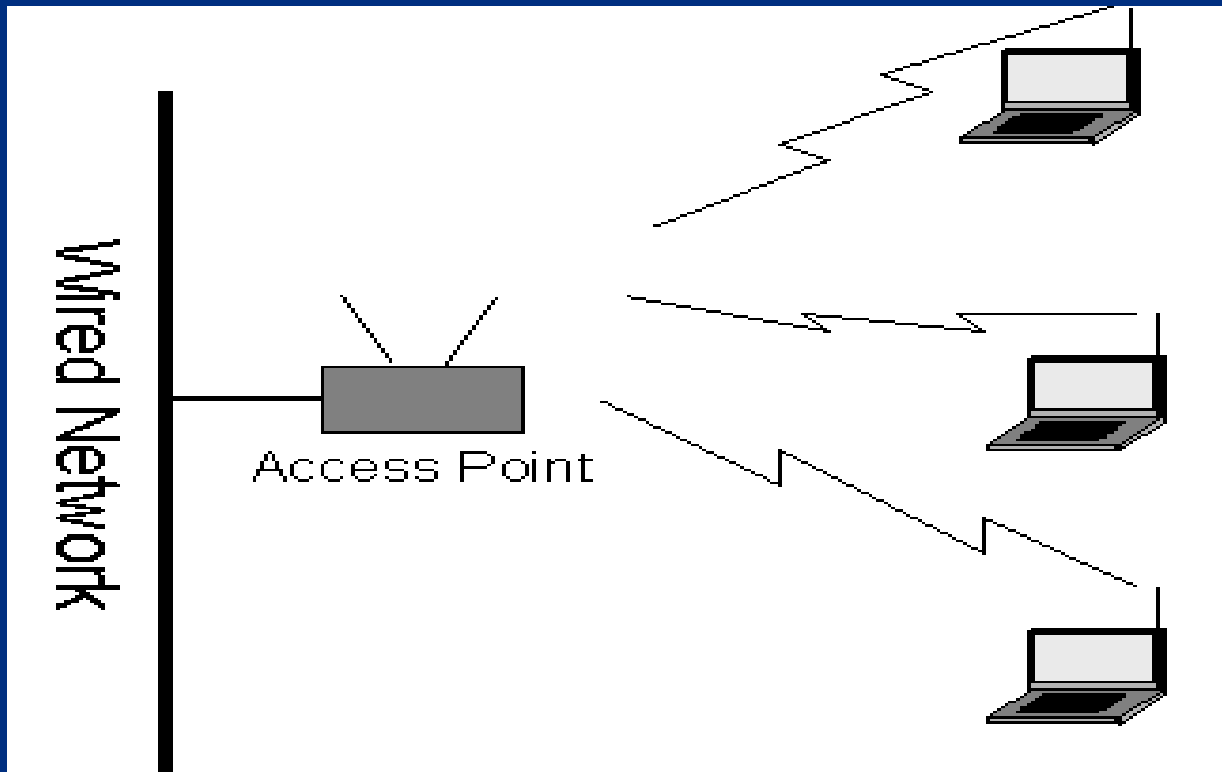
- Computers configured in infrastructure wireless network look for other wireless devices attached to wired network
- Devices, called access points, usually attached directly to hub or switch in wired network
- Primary function is to provide wireless computers with access to wired network
- Once connected to wired network, wireless devices can use resources available to wired network including Internet access



*U.S. Department of
Homeland Security*

United States
Secret Service

Infrastructure Wireless Network



*U.S. Department of
Homeland Security*

United States
Secret Service

Hardware Components

- A wireless local area network (WLAN) is rarely wireless
- Shared resources, such as Internet gateway, printers, file servers, etc., are typically all interconnected with cables



*U.S. Department of
Homeland Security*

United States
Secret Service

Wireless NIC

- Network interface card (NIC) is essential part of any wireless network
- Wireless NIC functions as interface between PC and media used to connect PC to network
- NICs typically have visible antennae as shown in examples on following slide



*U.S. Department of
Homeland Security*

United States
Secret Service

Wireless NIC Illustration



*U.S. Department of
Homeland Security*

United States
Secret Service

Wireless Access Points (WAP)

- Provides connection for Wireless NIC to wired network
- Generally small hardware device connected by cable to hub or switch on wired network
- Can also be wireless cable/DSL router that provides routing protection and functionality to broadband Internet service



*U.S. Department of
Homeland Security*

United States
Secret Service

Wireless Access Points (WAP)

- Usually equipped with one or two visible antenna
- Antennae receive signals from wireless NIC and converts to format compatible with cable that connects WAP to network
- Single WAP can support connections from multiple wireless devices



*U.S. Department of
Homeland Security*

United States
Secret Service

WAP Illustrations



*U.S. Department of
Homeland Security*

United States
Secret Service

Security Concerns

- Wireless network communications extremely vulnerable to eavesdropping and attack
- In broadcast network, data transmissions are sectioned into packets broadcast to all devices attached to network
- Packets broadcast over wireless connections can easily be intercepted and examined
- Data being transmitted can be viewed and reassembled by intercepting party



*U.S. Department of
Homeland Security*

United States
Secret Service

WEP

- Networking devices manufactured under 802.11 standards employ method of encryption called *wired equivalent privacy* or *WEP*
- Provides encryption of communications based on 64 or 128 bit key
- Wireless computer and WAP must use same key to communicate
- Wireless devices have ability to turn WEP on or off
- Default state of WEP for most devices is off



U.S. Department of
Homeland Security

United States
Secret Service

WEP

- WEP intended to secure wireless networks
- Flaws well documented
- Slightly better than no security at all
- With right combination of hardware and software WEP key can be cracked within minutes



*U.S. Department of
Homeland Security*

United States
Secret Service

WPA

- Wi-Fi Alliance, in cooperation with several members of IEEE 802.11i task group, developed Wi-Fi Protected Access (WPA) to address wireless security
- WPA uses dynamic keys so same encryption key never used twice
- WPA encryption key derived from up to 500 trillion possibilities
- Key virtually uncrackable if strong password used



*U.S. Department of
Homeland Security*

United States
Secret Service

LEAP

- Lightweight Extensible Authentication Protocol (LEAP) provides authentication services on wireless network
- When wireless client attempts to access network, wireless access point (WAP) blocks all ports except for authentication ports to allow input of authentication credentials
- Once received, WAP forwards credentials to special authentication server for validation
- If credentials valid, unique key generated for session and access to network through WAP is granted



*U.S. Department of
Homeland Security*

United States
Secret Service

LEAP

- Key generated is per-user and per-session, complicating and hopefully frustrating hacking attempts
- Time-out settings of key can be adjusted to force devices to re-authenticate frequently
- Re-authentication results in new session, new key
- Keys change frequently and sessions become short
- Packet sniffing becomes useless as means of deriving session keys



*U.S. Department of
Homeland Security*

United States
Secret Service

Service Set Identifier (SSID)

- Unique, user configurable name used to communicate with WAP
- Most wireless access points have SSID indicative of manufacturer or model of device
- Example, Linksys brand of WAP uses name LINKSYS as default SSID
- SSID can be any combination of alpha and numeric characters with maximum length of 32 characters



*U.S. Department of
Homeland Security*

United States
Secret Service

Service Set Identifier (SSID)

- When WAP powered on, begins broadcasting SSID to any wireless device within range
- Feature intended to simplify connectivity by mobile devices
- Can be disabled in some WAPs eliminating necessity for notebook PC or PDA users to know SSID before connecting



*U.S. Department of
Homeland Security*

United States
Secret Service

MAC Filtering

- Enabling WPA and MAC filtering are methods that can harden wireless network against attack
- If MAC filtering enabled, (disabled by default), list of MAC addresses is created for devices allowed to join network
- As connection attempts made, MAC address of each device validated against list
- Device denied access if device's MAC not on filter list
- Can be circumvented through MAC spoofing



*U.S. Department of
Homeland Security*

United States
Secret Service

Wireless Detection Systems

- Wireless detectors developed as result of security concerns
- Among solutions are small inexpensive detectors like examples shown on next slide
- Both devices cost less than \$25 and only detect presence of 802.11 wireless signals and signal strength
- Devices not well suited for determining WAP SSID, MAC address of WAP, or other information that can be detected using more sophisticated and expensive solutions



*U.S. Department of
Homeland Security*

United States
Secret Service

Wireless Detection Devices



*U.S. Department of
Homeland Security*

United States
Secret Service

Wireless Detection Systems

- Unauthorized or rogue wireless devices can appear on network for short durations, making them hard to detect
- Solution providers have developed detection systems comprised of specialized software and customized sensors to address issue
- Sensors placed strategically throughout network, constantly monitoring for rogue devices
- When device detected, location triangulated using strategically placed sensors



*U.S. Department of
Homeland Security*

United States
Secret Service

Wireless Detection Systems

- Once identified and approximate position determined, notebook computer or PDA equipped with directional antenna used to pinpoint device
- Can be accomplished by sweeping antenna in a 360-degree rotation while monitoring signal strength
- Number of freeware applications available to perform function
- Net Stumbler for MS Windows and Pocket PC, Kismet for Linux



*U.S. Department of
Homeland Security*

United States
Secret Service

War Driving Roots

- Hacker groups collaborated, developed software configured to search for BBS or modem-enabled mainframe computer by sequentially dialing telephone numbers within given area code and exchange
- As number dialed, hacker's computer waited for carrier signal of modem on other end
- No carrier detected, call ended and next number in sequence dialed
- If carrier detected, calling computer saved telephone number to log file, disconnect, moved to next number in sequence



*U.S. Department of
Homeland Security*

United States
Secret Service

War Driving

- Process called *war dialing* and became foundation for many hacking applications
- Concept was applied to wireless networks, but without modems
- Just as modems sat waiting for someone to connect, in wireless network, WAP waits
- Airwaves can be scanned for 802.11 signals, and SSIDs



U.S. Department of
Homeland Security

United States
Secret Service

War Driving

- Tools can be used with notebook computer to scan for and identify wireless networks
- Data these programs collect include:
 - SSID (if broadcasted)
 - Which of 14 wireless channels or frequencies used (only 11 used in U.S.)
 - Whether or not WEP or WPA is enabled
 - MAC address of WAP



*U.S. Department of
Homeland Security*

United States
Secret Service

War Driving

- Hackers have developed software similar to war dialer that attempts to connect to computers or WAPs
- Name War Driving derived from running programs on laptop with wireless NIC and external antenna while driving along major traffic routes in effort to locate wireless networks
- Common for War Drivers to record GPS coordinates of wireless networks for use with mapping software and for publication to various sites on Internet



*U.S. Department of
Homeland Security*

United States
Secret Service

Overlapping Signals

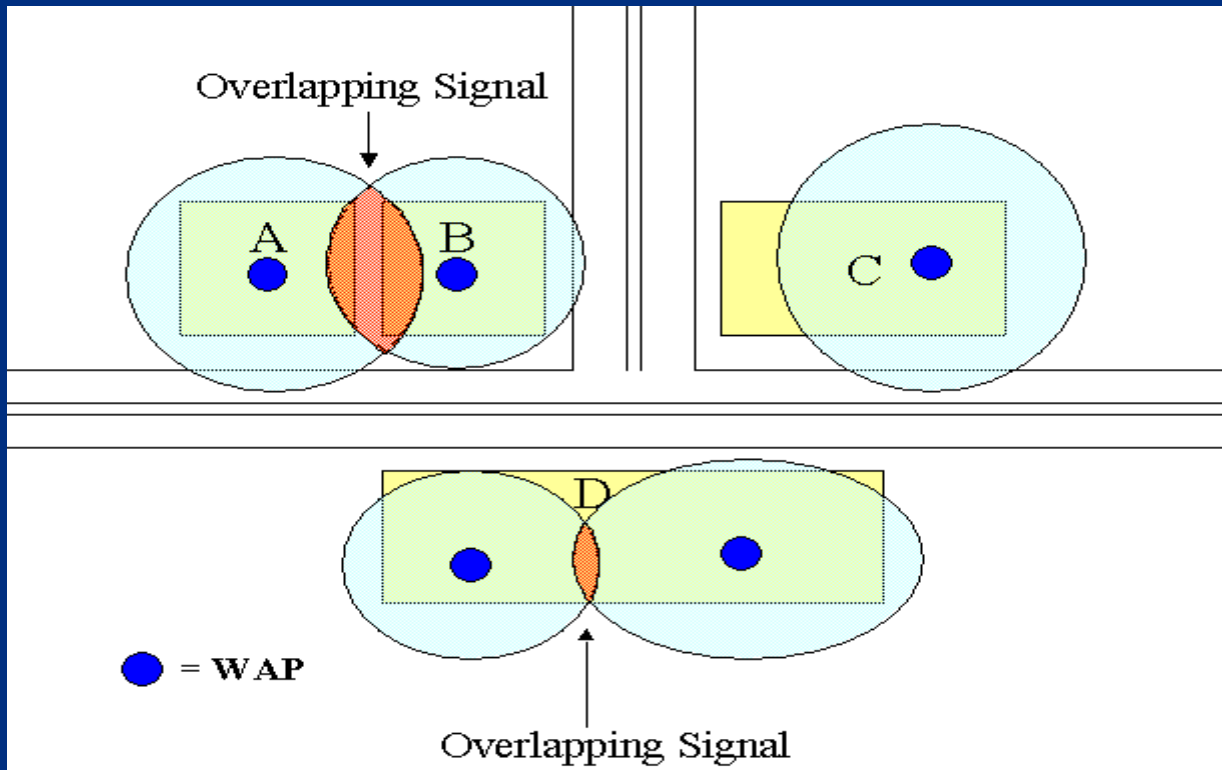
- Wireless network signals typically radiate in elliptical pattern
- Can vary depending upon physical structure in which WAP deployed
- Walls, floors, ceilings, and other obstacles affect radio waves



*U.S. Department of
Homeland Security*

United States
Secret Service

Overlapping Signals



U.S. Department of
Homeland Security

United States
Secret Service

Overlapping Signals

- Four buildings with wireless networks in illustration on previous slide
- Building C far enough away from other buildings, overlapping signals not an issue
- Building D has two wireless access points deployed with minimal signal overlap
- If two signals in building D are owned by different businesses, could pose a significant problem
- Buildings A and B wireless access points generate overlapping signals



*U.S. Department of
Homeland Security*

United States
Secret Service

Overlapping Corrective Action

- Relocation of the WAP
- Reducing power output of the WAP



*U.S. Department of
Homeland Security*

United States
Secret Service

Accidental Access

- Wireless end user operating in overlapping signal area could possibly connect to wrong network accidentally
- If wireless networks configured to use WEP, possibility of accidental access eliminated



*U.S. Department of
Homeland Security*

United States
Secret Service

Known Attacks

- Wireless network technology constantly improving
- There are known vulnerabilities that lead to attack
- Wireless network attacks usually result from improperly managed or improperly secured wireless technology



*U.S. Department of
Homeland Security*

United States
Secret Service

Session Hijacking

- Attacker monitors active sessions, connections between WAP and remote station, identifying information used to facilitate attack
- Once enough information collected, attacker sends spoofed message to target workstation to disconnect
- Workstation responds by ending session allowing attacker to masquerade as disconnected workstation



*U.S. Department of
Homeland Security*

United States
Secret Service

Man-in-the-Middle

- Exploits one-way authentication of 802.11 design, allows attacker to configure computer to act as wireless access point
- Attacker waits for users to connect to wireless network
- Remote computers pass WEP key to attacker's computer
- Attacker's computer connects to real WAP and passes remote computers packets transparently between user and WAP
- Result is captured WEP key that will allow attacker access to wireless network



*U.S. Department of
Homeland Security*

United States
Secret Service

WEP Key Cracking

- When WEP enabled, encrypted key used to connect to, and transfer data across wireless network
- Only computers with WEP key allowed to communicate
- Software tools, such as Aircrack-ng and WEPCrack, simplify job of cracking WEP key
- By monitoring packets transmitted across airwaves, attacker can save packets to log file
- After several thousand packets have been collected, cracking tools can analyze collected packets to determine WEP key



*U.S. Department of
Homeland Security*

United States
Secret Service

WPA-PSK Cracking

- WPA-PSK uses pre-shared key for its encryption algorithm
- Method much more secure than using WEP, but still susceptible to cracking
- Attack method used to crack WPA-PSK is dictionary attack
- Captured data between transmitting access point and user can be run through dictionary to find correct key to unlock data
- Countered by use of long key not found in dictionary, such as complete phrase with additional special characters, etc



*U.S. Department of
Homeland Security*

United States
Secret Service



*U.S. Department of
Homeland Security*

United States
Secret Service

Module 7 – IP Addresses and Subnets



*U.S. Department of
Homeland Security*

United States
Secret Service

You Will Learn . . .

- IP Addresses
- Ports
- Subnets
- Network Security



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 1 – IP Addresses

- IP Address Basics
- IP Address Classes
- More about IP Addresses



*U.S. Department of
Homeland Security*

United States
Secret Service

Network Addressing Overview

- In TCP/IP network, IP (Internet Protocol) addressing essential to physical routing of network communications
- Every device on LAN must have unique IP address
- Addresses essential for internetworking over WANs



*U.S. Department of
Homeland Security*

United States
Secret Service

Network Addressing Overview

- Media Access Control (MAC) address is unique hardware identification number specific for each network device
- To send data packet to host on LAN, sending device must first know receiver's MAC address
- MAC addresses exist at Data Link Layer 2 of OSI model



*U.S. Department of
Homeland Security*

United States
Secret Service

Network Addressing Overview

- IP addresses identify every device attached to TCP/IP network, including PCs, servers, switches, printers, and any other networked device
- Each device has unique IP address so it can be identified for internetwork data packet routing
- IP addresses exist at Network Layer 3 of OSI model



*U.S. Department of
Homeland Security*

United States
Secret Service

Network Addressing Overview

- Workstations can have permanent (static) IP address, or dynamically assigned address each time network connection established
- For clients on isolated LAN, administrator can assign unique static IP addresses
- To communicate with Internet, hosts must have unique registered Internet routable IP address



*U.S. Department of
Homeland Security*

United States
Secret Service

What's in an IP Address

- IP address, 32-bit numeric address written as four sets of numbers, called octets, separated by periods
- For example, 131.160.10.240 is example of class B IP address
- Each octet can range from 0 to maximum of 255
- Valid IP addresses cannot consist of all zeros or all ones



*U.S. Department of
Homeland Security*

United States
Secret Service

What's in an IP Address

- For each networked device, IP address consists of network address (netid) and host address (hostid)
- Each octet of IP address contains eight bits or one byte
- Address has total of four bytes



*U.S. Department of
Homeland Security*

United States
Secret Service

Example Class B IP Address

131.107.10.7

Typical Class B Internet Address 131.107.10.7

Bit # 0 31

10000011 . 01101011 . 00001010 . 00000111

131 107 10 7



*U.S. Department of
Homeland Security*

United States
Secret Service

Binary IP Addressing

- IP addresses read as set of four decimals
- Computer only reads ones and zeros
- IP addresses are binary, each of four decimals translated into eight binary numbers consisting of ones and zeros
- Binary numbering system used in IP addresses based on number 2, called Base2
- Each octet in address limited to eight bits, corresponding binary numbers range from 2^0 to 2^7 (1 to 255)



*U.S. Department of
Homeland Security*

United States
Secret Service

Converting Decimal 131 to Binary

Binary Conversion of Decimal 131								
Base2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Decimal	128	64	32	16	8	4	2	1
Binary Number is 10000011	1	0	0	0	0	0	1	1



*U.S. Department of
Homeland Security*

United States
Secret Service

Classes of IP Addresses

- IP addresses divided into several class types
- Class A, B, and C used for government and commercial addresses
- Class D and E reserved for multicasting, transmission of data to many recipients simultaneously
- Class D and E not commonly used
- Each class allows for specific maximum number of subnets and end nodes



*U.S. Department of
Homeland Security*

United States
Secret Service

Class A

Classes of IP Addresses Defined				
Class	First Octet	Maximum Networks	Maximum Hosts	Other Characteristics
A	1 – 126	126	16,777,214	Most often allocated to government and large institutions; Address Range: 1.X.X.X to 126.X.X.X



*U.S. Department of
Homeland Security*

United States
Secret Service

Class B

Classes of IP Addresses Defined				
Class	First Octet	Maximum Networks	Maximum Hosts	Other Characteristics
B	128 – 191	16,384	65,534	Most often allocated for commercial use and ISPs; Address Range: 128.X.X.X to 191.X.X.X



*U.S. Department of
Homeland Security*

United States
Secret Service

Class C

Classes of IP Addresses Defined				
Class	First Octet	Maximum Networks	Maximum Hosts	Other Characteristics
C	192 – 223	2,097,152	254	Most often allocated for commercial use and ISPs; Address Range: 192.X.X.X to 223.X.X.X



*U.S. Department of
Homeland Security*

United States
Secret Service

Class D

Classes of IP Addresses Defined				
Class	First Octet	Maximum Networks	Maximum Hosts	Other Characteristics
D	224 – 239	N/A	N/A	Reserved class used for multicasting; does not contain network or host IDs



*U.S. Department of
Homeland Security*

United States
Secret Service

Class E

Classes of IP Addresses Defined				
Class	First Octet	Maximum Networks	Maximum Hosts	Other Characteristics
E	240 – 247	N/A	N/A	Reserved class used for experimentation; does not contain network or host IDs



*U.S. Department of
Homeland Security*

United States
Secret Service

Reserved IP Addresses

Description	IP Address Range
Reserved for non-routable networks	<ul style="list-style-type: none">• 10.0.0.0 to 10.255.255.255• 172.16.0.0 to 172.31.255.255• 192.168.0.0 to 192.168.255.255
Reserved for loopback NIC testing	127.0.0.1



*U.S. Department of
Homeland Security*

United States
Secret Service

Reserved IP Addresses

Description	IP Address Range
Reserved for routing tables; refers to entire network	128.5.0.0
IDs an entire network	X.0.0.0 (Class A) X.X.0.0 (Class B) X.X.X.0 (Class C)
Broadcast	X.255.255.255 (Class A) X.X.255.255 (Class B) X.X.X.255 (Class C)



*U.S. Department of
Homeland Security*

United States
Secret Service

New Methods for IP Addressing

- Class system provides a finite number of IP addresses
- Number of unassigned Internet addresses running out
- New scheme called Classless Inter-Domain Routing (CIDR) introduced as replacement for system based on classes A, B, and C



*U.S. Department of
Homeland Security*

United States
Secret Service

Classless Inter-Domain Routing

- With CIDR, IP addresses assigned in blocks
- Single IP address can be used to identify many unique IP addresses
- CIDR IP address looks like normal IP address except it ends with a slash followed by a number
- End number is called IP prefix length, represents how many bits used for network partition of address
- An example of a CIDR address is 162.200.0.0/12



*U.S. Department of
Homeland Security*

United States
Secret Service

Classless Inter-Domain Routing

- Prefix length designates how many addresses available for network and hosts in CIDR address
- In example 162.200.0.0/12, first 12 bits of address identify network and remaining 20 bits identify host

10100010.1100|1000.00000000.00000000

$2^{12} = 4096$ Networks $2^{20} = 1,048,576$ Hosts per Network

- CIDR addresses also reduce size of routing tables and allows more IP addresses for subnetting and supernetting



*U.S. Department of
Homeland Security*

United States
Secret Service

IPv6

- Internet Protocol version 6 (IPv6), new method for IP addressing, significantly increases amount of available IP addresses
- Expands IP address from 32 bits to 128 bits
- Will provide over 3.4×10^{38} power new addresses
- Enough IP addresses that every cell of human body could be assigned one with addresses to spare



*U.S. Department of
Homeland Security*

United States
Secret Service

IPv6

- Addresses presented in hexadecimal format, such as:

FE80:325B:134C:5555:678D:9C4D:3EEE:2D5F

- Format consists of eight groups of hexadecimal digits
- Initially, many addresses will have zeros in groups



*U.S. Department of
Homeland Security*

United States
Secret Service

IPv6

- Shorthand notation exists to express groups of zeros, :: (the colon-colon operator)
- All groups in colons are zeros
- For example, IPv6 address, FE80::3E4F
 - First group is FE80
 - Second through 7th groups are all zeros
 - Eighth group is 3E4



*U.S. Department of
Homeland Security*

United States
Secret Service

IPv6 Special Addresses and Prefixes

Address	Description
::FFFF:0:0/96	Used for IPv4 mapped addresses
FC00::/7	Unique local IPv6 unicast addresses. Routable only within set of cooperating sites. Replaced “site-local” used in earlier implementation of IPv6.



*U.S. Department of
Homeland Security*

United States
Secret Service

IPv6 Special Addresses and Prefixes

Address	Description
FE80::/10	Local link for use within a LAN. Similar to 169.254.x.x, the autoconfig IP address in IPv4.
FF00::/8	Multicast prefix. No address ranges reserved for broadcast. Applications are to use multicast.



*U.S. Department of
Homeland Security*

United States
Secret Service

IPv6 Special Addresses and Prefixes

Address	Description
::1 /128	Loopback or “localhost” address. Similar to 127.0.0.1 IPv4 loopback address.
FE80::/10 through FEB0::/10	Private address ranges. Similar to IPv4 private LAN addresses. Local link addresses. Stateless and autoconfigured for use within LAN segment.



*U.S. Department of
Homeland Security*

United States
Secret Service

IPv6 Special Addresses and Prefixes

Address	Description
FEC0::/10 through FEF0::/10	Private address ranges. Similar to IPv4 private LAN addresses. Local site addresses.
FF00::/8 prefix	Multi-cast prefix
(2000 to 3FFF)::/16 prefix	Global unicast prefix



*U.S. Department of
Homeland Security*

United States
Secret Service

IPv6 Special Addresses and Prefixes

Address	Description
2001::/16	Assigned to Regional Internet Registrar (RIR)
2002::/16	Assigned to 6to4 Transition Methods
3FFE::/16	Temporary address assigned to 6bone



*U.S. Department of
Homeland Security*

United States
Secret Service

Dual Stacks

- Routers and computers can be configured to use both IPv4 and IPv6
- Routers that route both IPv4 and IPv6 packets called dual-stack
- No need for subnet mask address or NAT (Network Address Translation) with IPv6, although NAT can be implemented



*U.S. Department of
Homeland Security*

United States
Secret Service

Pseudo-Interfaces

- Network card can be configured with multiple IPv6 addresses
- For example, one address can be for just a segment, another for the site, and third can be for Internet
- IPv6 protocol assigns pseudo-interfaces or zone IDs for each of these
- An address may look like ABCD::1234:B2C3 %4
 - %4 would be its zone ID



*U.S. Department of
Homeland Security*

United States
Secret Service

Domain Name Service

- Most networks and Web sites have text-based domain names people can remember, such as www.google.com
- Internet based on numerical IP addresses
- Domain name service (DNS) translates text domain names into numerical IP addresses before Internet connection made
- Type Web address to favorite site, DNS server receives site request and translates into corresponding IP address



*U.S. Department of
Homeland Security*

United States
Secret Service

Dynamic Host Configuration Protocol

- Dynamic Host Configuration Protocol (DHCP) used to assign dynamic IP addresses to devices on network
- Addresses are assigned from pool of pre-registered addresses
- Eliminates need and time to manually assign IP addresses to new network equipment
- Tracks all assigned addresses automatically



*U.S. Department of
Homeland Security*

United States
Secret Service

Dynamic Host Configuration Protocol

- Computer or other device can be assigned different IP address every time it accesses network
- Device can change IP address between logon and logoff
- ISPs frequently use DHCP for dial-up and broadband users
- DHCP6 will run in networks that have implemented IPv6



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 2 – Ports

- Overview of Ports
- How Ports are Used
- Configuring TCP/IP



*U.S. Department of
Homeland Security*

United States
Secret Service

Ports

- Communications over computer networks similar to telephone system in sense that thousands of conversations between computers occur every second
- For computers and applications to communicate, need means of channeling communications, called service ports, or simply *ports*



U.S. Department of
Homeland Security

United States
Secret Service

Ports

- When computer receives data from network, TCP/IP protocol stack must know data's user application destination
- For example, Web server sends Web page to computer, TCP/IP must know Web page data goes to Web browser to display page



*U.S. Department of
Homeland Security*

United States
Secret Service

Ports

- TCP/IP maps data to an application using a port, number that represents an application
- Each transmission is labeled with source and destination port
- The source port identifies application sending data
- Destination port identifies application to process data



*U.S. Department of
Homeland Security*

United States
Secret Service

Well-Known Ports

- Over 65,000 ports available to network applications
- Ports 1 – 1023 usually map to specific applications, regardless of computers involved
- For this reason, they are often called *well-known ports*



U.S. Department of
Homeland Security

United States
Secret Service

Well-Known Ports

Service	Protocol	Port Number
World Wide Web (HTTP)	TCP	80
Telnet	TCP	23
Simple Mail Transfer Protocol (SMTP)	TCP	25
File Transfer Protocol (FTP) Control	UDP	21



*U.S. Department of
Homeland Security*

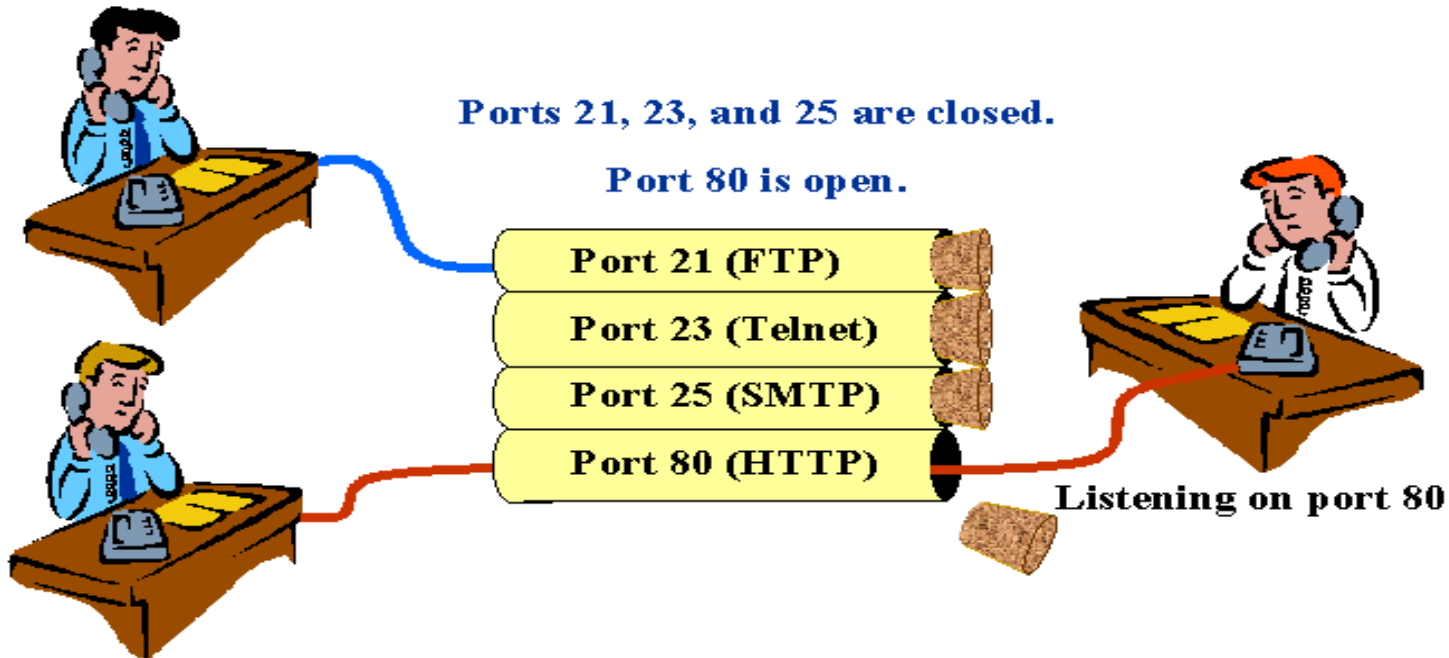
United States
Secret Service

Communication Through Ports

Talking on port 21

Ports 21, 23, and 25 are closed.

Port 80 is open.



Talking on port 80



*U.S. Department of
Homeland Security*

United States
Secret Service

Port Use

- Network hardware devices such as firewalls, routers and gateways offer ability to close or open certain ports
- Provides or denies access to specific types of information
- Some network devices can open port, but restrict packets traveling through port
- For example, port 21 (File Transfer Protocol) can be opened, but monitored to disallow packets carrying the put command
- Conversely, the get command would not be blocked



*U.S. Department of
Homeland Security*

United States
Secret Service

Port Management

- Computer's ports can be enabled or disabled using features of operating system
- Windows XP, for example, provides built-in software firewall that automatically restricts port access
- Terminating an active service on server can also disable ports
- Example, FTP service can be disabled using features of operating system, disabling port 21



*U.S. Department of
Homeland Security*

United States
Secret Service

Port Management

- Often, ports managed through configuration of hardware firewalls
- Hardware firewalls can be managed locally by attaching special cable from PC to network device and running standard communications software, such as Telnet or HyperTerminal
- Devices can be managed remotely with Telnet
- Can be managed through Web browser, such as Internet Explorer, pointing browser to device's IP address



*U.S. Department of
Homeland Security*

United States
Secret Service

Port Management

- Regardless of management technique, device will most likely have administration account requiring login ID and password to configure device
- Windows XP firewall has rules that block inbound communication attempts
- Windows Vista firewall includes rules that block both inbound and outbound communication attempts



*U.S. Department of
Homeland Security*

United States
Secret Service

Port Misuse

- Most government agencies and corporations publish policies specifying port configurations for network devices
- Blocking certain ports mandatory in many instances
- Policies intend to minimize risk of intrusion standard
- Technical personnel might “bend the rules” to accomplish specific task and open unauthorized port on network device long enough to accomplish task
- Policies protecting network violated and network becomes vulnerable



*U.S. Department of
Homeland Security*

United States
Secret Service

Procedure: Create a TCP/IP LAN via a Router with Microsoft Vista

- This is a Step / Action in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 3 – Subnets

- Subnet Overview
- Subnet Masks
- Virtual LAN



*U.S. Department of
Homeland Security*

United States
Secret Service

Subnets

- Class A, B, and C networks can be subdivided into subnets
- *Subnet* is segment of network that shares common IP network address component with other devices on same subnet
- Devices with same IP address prefix belong to same subnet on TCP/IP network
- Networks on Internet view other networks as single entities
- No way of viewing another network's subnet structure, helps reduce size of routing tables



U.S. Department of
Homeland Security

United States
Secret Service

Subnets

- When data packet is sent over Internet, it goes to router of destination network
- Router determines destination node by deciphering packet's subnet address



*U.S. Department of
Homeland Security*

United States
Secret Service

Advantages of Subnetting

- Enhances security by creating subnets that have restricted access
- Extends capabilities of network
- Enhances network performance, eliminating traffic on other segments



*U.S. Department of
Homeland Security*

United States
Secret Service

Advantages of Subnetting

- Allows subnets to be invisible to outside world
- Provides flexibility to deploy additional subnets without registering new network numbers
- Allows data route changes within network without affecting Internet routing table



*U.S. Department of
Homeland Security*

United States
Secret Service

Subnet Addressing

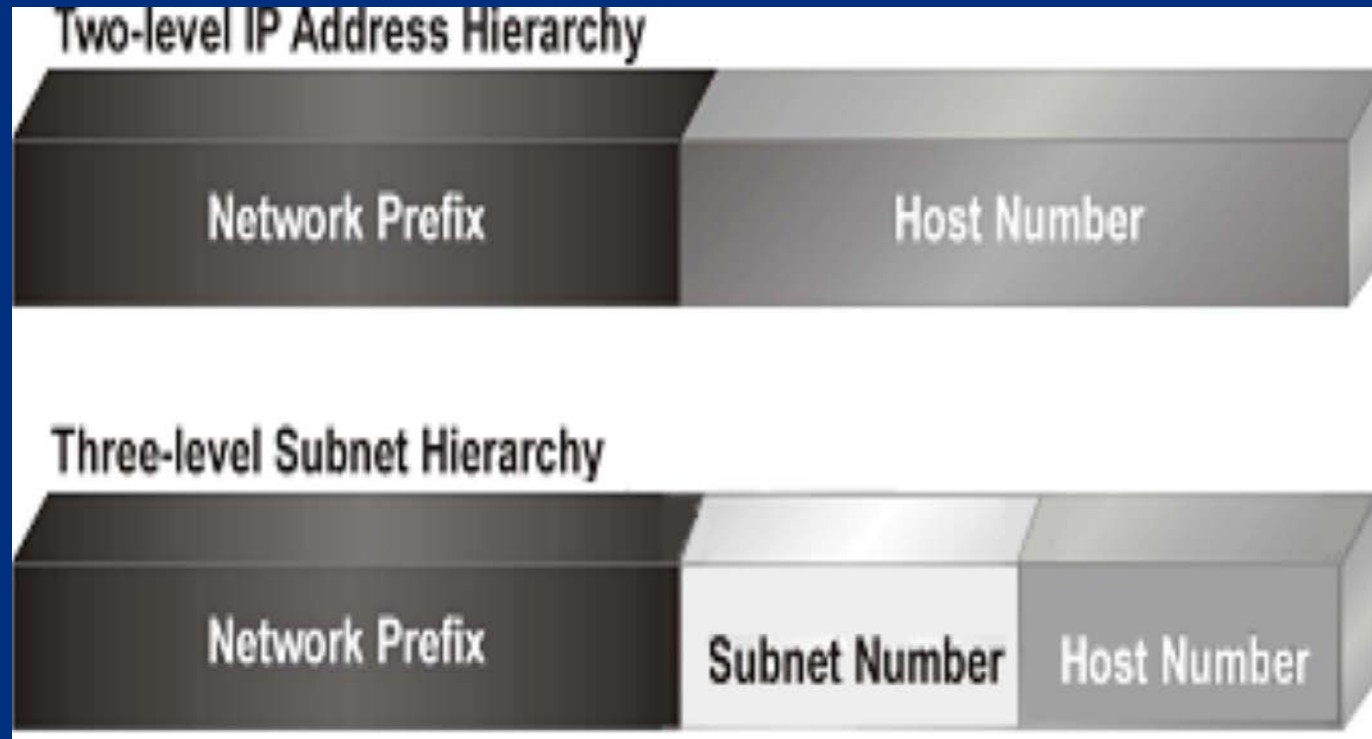
- Like IP addresses, each subnet address is unique
- Recall each IP address has four octets, address divided into two major segments: network and host
- By comparison, subnet address contains three segments: network address, subnet address, host address



*U.S. Department of
Homeland Security*

United States
Secret Service

IP Address vs. Subnet Address



*U.S. Department of
Homeland Security*

United States
Secret Service

Creating Subnets

- Subnets created as extensions of network number
- To create, take bits from host number and reassign to subnet field
- The more bits taken from host number, the fewer host addresses that can be assigned to subnet



*U.S. Department of
Homeland Security*

United States
Secret Service

Subnet Masks

- A *subnet mask* conceals a subnet from outside networks
- Two main functions of a subnet mask:
 - Identify subnet of an IP address
 - Notify communicating devices which part of IP address is network ID (including subnet) and which part is host ID



U.S. Department of
Homeland Security

United States
Secret Service

Default Classes of Subnet Masks

- Class A - 255.0.0.0
- Class B - 255.255.0.0
- Class C - 255.255.255.0



*U.S. Department of
Homeland Security*

United States
Secret Service

Subnet Masks Components

- Subnet masks use same 32-bit, four-octet structure as IP addresses
- Subnet mask addresses have three parts: network address, subnet address, host address
- Subnet mask has all ones in network and subnet segments of address and contains all zeros in host segment
- With subnetting, part of host address used to identify subnet
- Subnet mask is network address plus bits reserved to identify subnet



*U.S. Department of
Homeland Security*

United States
Secret Service

Virtual LAN

- Virtual LAN (VLAN), another way to divide local area network into logical subgroups
- VLAN uses software to connect group of computers and devices instead of manually moving cables and wiring
- Can be used to combine workstations and other devices into single group regardless of physical location
- Improves traffic flow within workgroup



*U.S. Department of
Homeland Security*

United States
Secret Service

Virtual LAN

- VLANs used in LAN switches
- Network changes and additions quickly implemented with VLAN software making group solutions easy to create
- VLANs operate at Data Link Layer 2 and Network Layer 3 of OSI model



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 4 – Network Security

- Data Encryption
- Anti-Virus Software
- Firewalls
- IDS
- Logs
- Network Security Summary



*U.S. Department of
Homeland Security*

United States
Secret Service

Data Encryption

- Conversion of data into form that cannot be easily deciphered
- Encrypted text called cipher text
- Decryption converts encrypted data into plain text
- Encryption provides highly effective method for data protection



*U.S. Department of
Homeland Security*

United States
Secret Service

Two Types of Encryption

- *Asymmetric encryption* uses two types of cryptographic keys to encode messages
 - Public key is known to everyone
 - Private key is only known to recipient
 - Method works because public key relates to private key so that messages can be decrypted upon receipt
- *Symmetric encryption* uses same key to encode and decode messages



U.S. Department of
Homeland Security

United States
Secret Service

Virus

- Small piece of code that executes when opening a real program or file
- Example, virus might attach itself to word processing file
- When file opened, virus code attaches itself to word processing program
- Each time program runs, virus runs
- Has chance to replicate by attaching to other programs or wreak havoc, such as deleting entire contents of hard drive



*U.S. Department of
Homeland Security*

United States
Secret Service

E-mail Viruses

- Spreads in e-mail messages
- Usually automatically mails itself to every address in victim's e-mail address book



*U.S. Department of
Homeland Security*

United States
Secret Service

Worms

- Small piece of code uses computer networks and vulnerabilities, known as security holes, to replicate itself
- Worm scans network for any machine that has specific security hole
- Copies itself to new machine using security hole, and starts replicating from there



*U.S. Department of
Homeland Security*

United States
Secret Service

Trojan Horses

- A computer program, not a virus
- Program claims to do one thing, instead could do deliberate damage when run
- For example, Trojan horse may claim to be a game, but instead may erase hard disk or create “back door”
- Trojan horses have no way to replicate automatically



*U.S. Department of
Homeland Security*

United States
Secret Service

Boot Sector Viruses

- Boot sector viruses spread by infecting boot sector of boot media, usually hard drive or floppy diskette
- Once infected, every time computer boots, virus is loaded automatically into memory
- Thereafter, attempts to infect every other program and file opened



*U.S. Department of
Homeland Security*

United States
Secret Service

Firewalls

- Method of securing a network from unauthorized access
- Most often, protect against intruders who seek access via Internet
- Enterprises install firewalls to secure Internet access for employees, separate and protect intranet from unauthorized public Web site traffic
- Also installed to protect organization's internal departments or domains, such as firewall that secures accounting department



*U.S. Department of
Homeland Security*

United States
Secret Service

Firewalls

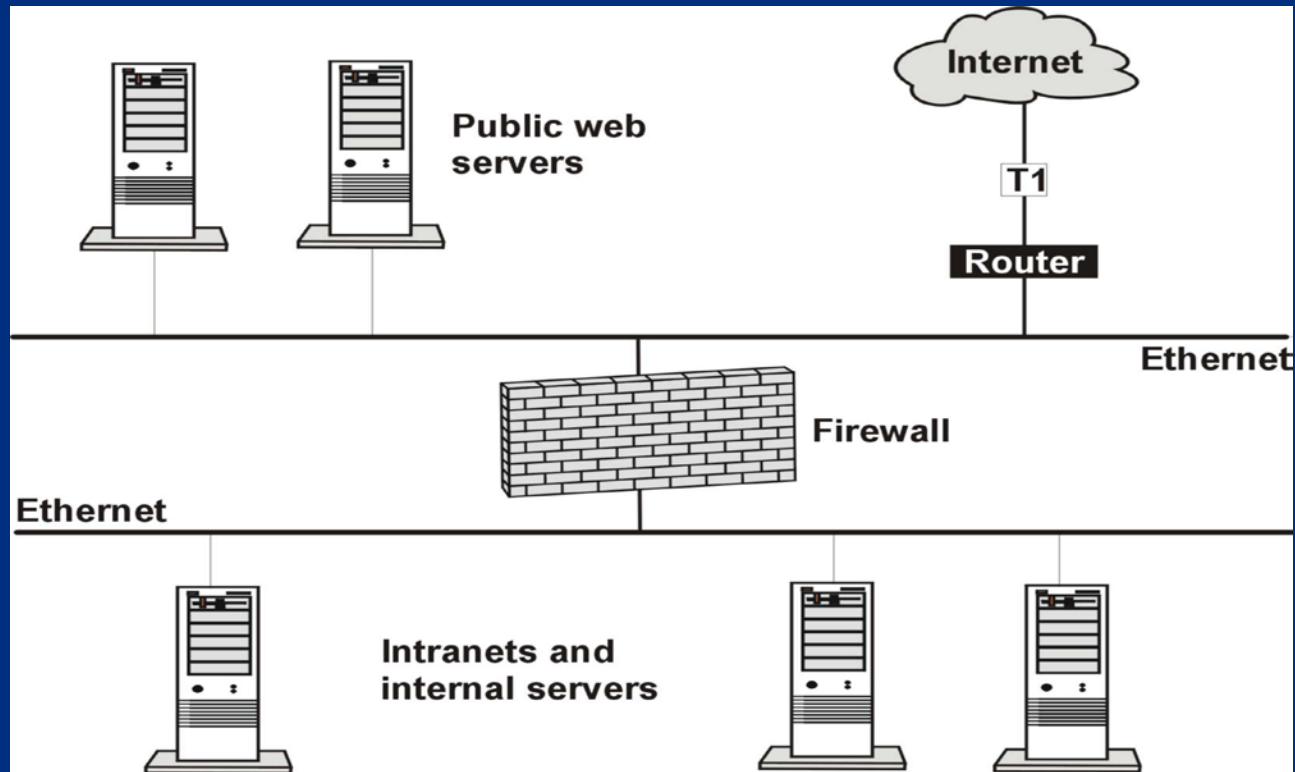
- Protection can be software, hardware, or combination of both
- Each performs specific security activities
- Firewalls are access control devices that only detect failed attempts at access
- If intruder defeats corporate firewall, intrusion may or may not be logged, depending on firewall configurations



*U.S. Department of
Homeland Security*

United States
Secret Service

Intranet Protected by Firewall



*U.S. Department of
Homeland Security*

United States
Secret Service

How Firewalls Work

- All messages going in or out of the network pass through firewall
- Messages checked using specified security criteria
- Firewall blocks those that do not meet criteria
- Different types of firewalls work at various layers of OSI model or TCP/IP protocol



*U.S. Department of
Homeland Security*

United States
Secret Service

Network Address Translation (NAT)

- NAT allows use of internal non-routable IP addresses on intranet to connect to Internet with one registered IP address
- Registered IP address assigned to software or hardware device running NAT
- Process allows any computer behind NAT device to be invisible to Internet
- Only NAT device's registered IP address is used



*U.S. Department of
Homeland Security*

United States
Secret Service

How NAT Works

- Intranet computer sends data packet to NAT device
- NAT device examines packet header and records intranet computer making request
- NAT device replaces IP address with its own registered IP address and sends request to Internet
- When packet returns, it goes to IP address of NAT device
- NAT device examines packet, places appropriate IP address for intranet computer in packet, and sends to computer



*U.S. Department of
Homeland Security*

United States
Secret Service

Stateful Inspection

- *Stateful inspection* firewall architecture has ability to look into packet and allow only certain types of application commands while rejecting others
- For example, stateful packet-filtering firewall allows FTP command Get and rejects Put command



U.S. Department of
Homeland Security

United States
Secret Service

Stateful Inspection

- Stateful inspection firewalls record User Datagram Protocol (UDP) packet requests permitted to cross firewall in state table
- Incoming UDP packets examined and verified against ones waiting for response in state table
- If information matches, request is permitted to enter network, otherwise packet rejected



*U.S. Department of
Homeland Security*

United States
Secret Service

Packet-filtering Firewalls

- *Packet-filtering* firewalls check header of packets for specific information and accepts or rejects packets based on user-defined rules
- Checks are made for:
 - Source and destination IP address
 - Source and destination port numbers
 - Protocol type
 - Direction of the packet (inbound or outbound)



U.S. Department of
Homeland Security

United States
Secret Service

Packet-filtering Firewall Advantages

- Good performance
- NAT shields internal addresses from external users
- No code modifications are needed
- Closes ports when not in use
- Stateful inspection checks packets and only allows those through that were requested



*U.S. Department of
Homeland Security*

United States
Secret Service

Packet-filtering Firewalls

Disadvantage

- Subject to IP spoofing or port spoofing
- Cannot filter or authenticate URL information
- Little or no auditing or alert mechanisms
- Rules need to be entered for stateful inspection type firewalls and then changed



*U.S. Department of
Homeland Security*

United States
Secret Service

Circuit-level Firewall

- Validates TCP and UDP sessions before opening connection
- After validation, passes everything through until session ends
- Establishes a virtual circuit between client and host on session-by-session basis
- Maintains table of connections including session and sequencing information
- When session ends, table information removed and virtual connection is closed



*U.S. Department of
Homeland Security*

United States
Secret Service

Circuit-level Firewall

- Only packets associated with session are allowed through
- If packet is valid according to session table, packet is passed through without any further security checks
- Session consists of two connections: one between client and firewall and one between firewall and server
- All outgoing packets appear to have originated from firewall in method similar to NAT



*U.S. Department of
Homeland Security*

United States
Secret Service

Circuit-level Firewall Advantages

- Good performance because packets are not examined after initial connection is allowed
- No direct connection between client and application server
- Similar to NAT's method of shielding internal IP address



*U.S. Department of
Homeland Security*

United States
Secret Service

Circuit-level Firewall Disadvantages

- Client programs need to be recompiled and relinked to a special library containing set of rules for sessions
- Does not examine application level information in packets allowing them to be subverted by inside user or outside hacker



*U.S. Department of
Homeland Security*

United States
Secret Service

Application-Gateway Firewall

- Runs on proxy server application that acts as intermediary between two systems
- Evaluates all requests from internal computers to connect to external service, such as FTP
- Determines whether to permit or deny request based on rules defined for individual network



*U.S. Department of
Homeland Security*

United States
Secret Service

Application-Gateway Firewall

- Application-gateway running on proxy server understands protocols of service it is evaluating
- Can deny packets that do not comply with protocol for service
- Provides detailed audit records or session information, user authentication, URL filtering, and caching



*U.S. Department of
Homeland Security*

United States
Secret Service

Application-Gateway Firewall

- Application-gateway firewalls are application specific and require proxy addresses for FTP, HTTP, SMTP, etc
- These firewalls operate at Application Layer of OSI model
- Able to look down through packets to application layer information to determine if packet is altered or not complying with appropriate protocol rules
- Additional steps cause application-gateway firewall to be slower than other types of firewalls



*U.S. Department of
Homeland Security*

United States
Secret Service

Application-Gateway Firewall Advantages

- No direct connection between internal client and external server
- Can deny packets that do not comply with protocol for service, such as FTP, HTTP, SMTP, etc
- Ability to screen data streams for potential threats, such as send mail attacks, and Java or ActiveX scripts riding on top of HTTP services
- Provide NAT services



*U.S. Department of
Homeland Security*

United States
Secret Service

Application-Gateway Firewall Advantages

- Transparent to individual user
- Can implement features such as HTTP object caching, URL filtering and user authentication
- Provide audit logs for administrators to monitor for violations of security policy



*U.S. Department of
Homeland Security*

United States
Secret Service

Application-Gateway Firewall Disadvantages

- Slower than other firewall methods
- Vulnerable to operating system and application level bugs because highly dependant on operating system, TCP/IP stacks, and runtime libraries
- New services require new proxy servers



*U.S. Department of
Homeland Security*

United States
Secret Service

Intrusion Detection Systems (IDS)

- Monitor network for attacks
- Two basic types of IDSs:
 - *Network-based IDS* monitors entire network for signs of intrusion
 - *Host-based IDS* monitors individual computer
- IDS must be installed consistent with network's type and topology



U.S. Department of
Homeland Security

United States
Secret Service

Network-based IDS

- Monitors entire network and uses information in data packets to detect intrusion
- Analyzes packets for *attack signature*, known pattern in packet or packets that match specific attack type
- Analyzes packets in real time using recognition files
- Most common method used by IDS pattern expression is byte code matching, also known as signature analysis or misuse detection



U.S. Department of
Homeland Security

United States
Secret Service

Network-based IDS

- When attack identified, IDS can be programmed to perform any of following actions:
 - Send alert to console
 - Log event and send email
 - Initiate connection kill (TCP reset)
 - Reconfigure firewall or router, or use SNMP trap
- Important to keep list of known attack signatures current



*U.S. Department of
Homeland Security*

United States
Secret Service

Host-based IDS

- Host-based IDS installed on individual computer to monitor only that computer
- Host-based IDSs are used to:
 - Monitor logs
 - Detect file access
 - Detect attempts to install executables
 - Monitor remote user activities



*U.S. Department of
Homeland Security*

United States
Secret Service

Host-based IDS

- Specific to OS installed on computer
- On host with NT OS, IDS will monitor system, event, and security logs
- On host with Unix OS, IDS will monitor syslog
- Host-based IDS examines each log's entry to see if it matches any known attack pattern
- Some can monitor ports on computer
- Can also detect attacks initiated from local keyboard



*U.S. Department of
Homeland Security*

United States
Secret Service

Host-based IDS Actions

- Log event
- Alert console and send an e-mail
- Initiate a SNMP trap
- Terminate user login and disable user account



*U.S. Department of
Homeland Security*

United States
Secret Service

Logs

- Record of network activity that provide details of transactions and traffic
- Routinely used for backup, recovery, and statistical purposes
- Also used to detect failed and successful intrusions, abnormal network activity, and system activities
- Many different types of logs generated by both software and hardware devices
- Can be integral part of computer forensic investigations



*U.S. Department of
Homeland Security*

United States
Secret Service

Common Logs

- System logs
- Firewall logs
- Router logs
- IDS logs



*U.S. Department of
Homeland Security*

United States
Secret Service

System Logs

- Most networking operating systems able to maintain log files
- Can include system activities, application activities, and security activities
- Most systems can be configured to maintain logs for Internet access, FTP sessions, etc



*U.S. Department of
Homeland Security*

United States
Secret Service

System Logs

- Example, Windows NT/2000/XP maintains three main logs that can be accessed through Event Viewer
 - System log
 - Security log
 - Application log



*U.S. Department of
Homeland Security*

United States
Secret Service

Firewall Logs

- Type of attempted access (Web access, FTP access, Telnet access etc.)
- Port that attempted access
- Date and time of attempted access
- IP address from which attempt came
- Application-level firewall logs can also provide detailed information of session information, user authentication, and security policy violations



*U.S. Department of
Homeland Security*

United States
Secret Service

Router Logs

- Can log information about network traffic and potential network problems
- Can be configured to log abnormal activity that contains host information of possible intruder and what was accessed on network during attempt
- Dial-up-access routers, can log dial-up connection information including username, IP address assigned, date, time, duration of connection
- Can be very beneficial during an intrusion investigation



*U.S. Department of
Homeland Security*

United States
Secret Service

IDS Logs

- Intrusions
- Intrusion attempts
- Unauthorized access to a computer
- Attempts to access unauthorized data
- Attempts to manipulate privileged files
- Attempts to render a network system inoperable



*U.S. Department of
Homeland Security*

United States
Secret Service

Network Security Summary

- Layered approach commonly used
- Intrusion Detection to provide real-time monitoring of network
- Firewalls to restrict unauthorized access to network
- Anti-virus protection to reduce risk of infection
- Encryption to prevent stolen data packets from being read
- Logs to record activity and provide documentation should a breach of security occur



*U.S. Department of
Homeland Security*

United States
Secret Service



*U.S. Department of
Homeland Security*

United States
Secret Service

Module 8 – Common Network Crimes



*U.S. Department of
Homeland Security*

United States
Secret Service

You Will Learn . . .

- E-Mail Scams
- On-line Fraud
- Identity Theft
- Social Threats
- Internal Threats



*U.S. Department of
Homeland Security*

United States
Secret Service

You Will Learn . . .

- Malicious Code
- Denial of Service Attacks
- Extortion
- Network Attacks
- Terrorism



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 1 – E-Mail Scams

- Overview
- Attack Methodologies
- Investigative Response



*U.S. Department of
Homeland Security*

United States
Secret Service

E-Mail Scams

- Scam defined as a dishonest act or fraud
- Postal system used for fraudulent means since the 1660's
- Simple step for surface-mail scammers to make leap to Internet E-mail



*U.S. Department of
Homeland Security*

United States
Secret Service

Why E-mail Scams Works

- People do not look closely at e-mail header information
- Few notice or question origin of messages
- Some scams use HTML encoded E-mail to display logos and other items to give impression of respectability
- Easy to hide code in HTML formatted E-mail that launches Trojans or other malicious code when E-mail viewed
- Chain E-mails and solicitations for money using every imaginable story and trick are prevalent on Internet



*U.S. Department of
Homeland Security*

United States
Secret Service

Nigerian, or 419 Scam

- Legendary among E-mail frauds
- Virtually all originate from foreign countries that have no agreement with U.S. pertaining to prosecution of fraud
- Person making request claims to be government official, or relative of deposed leader or potentate
- Requests involve large, usually multi-million dollar, sums of money
- Tap into greed of recipient



*U.S. Department of
Homeland Security*

United States
Secret Service

Nigerian, or 419 Scam

- Reason person making request can't get money themselves, but recipient, being an upstanding American can
- Will ask sum of money be deposited in account in other country
- Transfers of money to foreign account
- Requestor absconds with money
- Perpetrator outside reach of U.S. Law Enforcement



*U.S. Department of
Homeland Security*

United States
Secret Service

Where 419 Comes From

- Nigerian government has taken hard line against frauds
- Section 419 of Nigerian Criminal Code outlaws activity
- Nigerian Government also considers anyone trying to remove funds from their country a criminal
- Victims who have gone to Nigeria to try get money back have been imprisoned



*U.S. Department of
Homeland Security*

United States
Secret Service

Phishing

- Perpetrator sends out legitimate looking E-mail in attempt to gain financial or personal information
- Compromised information used for other network crimes
- E-Bay/PayPal
- Banks
- Cross Site Scripting



*U.S. Department of
Homeland Security*

United States
Secret Service

Spam

- Unsolicited advertisement or bulk E-mail
- Use of network bandwidth consumed
- Storage space on mail servers
- Estimated cost to companies in U.S. is over \$12 billion dollars a year



*U.S. Department of
Homeland Security*

United States
Secret Service

E-mail Scam Investigative Response

- Capture
- Preservation
- Warrants
- Reporting
- Education



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 2 – Online Fraud

- Overview
- Attack Methodologies
- Investigative Responses



*U.S. Department of
Homeland Security*

United States
Secret Service

Online Fraud

- Any form of trickery or deceptive gain practiced on Internet



*U.S. Department of
Homeland Security*

United States
Secret Service

Common Attack Vectors

- Price too good to be true
- Short time to decide
- Fine print
- Hijacked sites
- Box-of-rocks
- Stall tactics



*U.S. Department of
Homeland Security*

United States
Secret Service

Attack Methodologies

- Bogus web sites
- Auctions
- Bogus Charities



*U.S. Department of
Homeland Security*

United States
Secret Service

Investigative Responses

- Capture
- Preservation
- Warrants
- Reporting
- Education
- Recording Observations



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 3 – Identity Theft

- Overview
- Attack Methodologies
- Investigative Responses



*U.S. Department of
Homeland Security*

United States
Secret Service

Identity Theft

- In 2007 estimated 8.4 million reported cases of identity theft in U.S.
- Number down from reported 10.1 million in 2003
- Even with decline identity theft problem is major problem



*U.S. Department of
Homeland Security*

United States
Secret Service

Gathering Personal Information

- Search Engines
- Public information sites
- Group sites
- Commercial sites
- Membership sites



*U.S. Department of
Homeland Security*

United States
Secret Service

Attack Methodologies

- Name
- Phone
- Social Security Number
- Address
- License plate



*U.S. Department of
Homeland Security*

United States
Secret Service

Attack Methodologies

- Pretexting – using small bits of information about subject to gather more details from businesses and vendors
- Attacker calls business or service that victim is member of and pretends to be victim
- Using information already gathered, attacker persuades business to disclose further information, or change information in account of victim to allow attacker full control of account



*U.S. Department of
Homeland Security*

United States
Secret Service

Investigative Responses

- Capture
- Preservation
- Warrants
- Reporting
- Education



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 4 – Social Threats

- Overview
- Attack Methodologies
- Investigative Responses



*U.S. Department of
Homeland Security*

United States
Secret Service

Social Threats

- Predators
- Stalkers
- Cyberbullying



*U.S. Department of
Homeland Security*

United States
Secret Service

Attack Methodologies

- E-mail
- Chat
- Texting
- Impersonation



*U.S. Department of
Homeland Security*

United States
Secret Service

Investigative Responses

- Capture
- Preservation
- Warrants
- Reporting
- Education



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 5 – Internal Threats

- Overview
- Attack Methodologies
- Investigative Responses



*U.S. Department of
Homeland Security*

United States
Secret Service

Internal Threats

- Inappropriate Usage
- Embezzlement
- Extortion
- Espionage
- Sabotage



*U.S. Department of
Homeland Security*

United States
Secret Service

Investigative Responses

- Capture
- Preservation
- Warrants
- Reporting
- Education



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 6 – Malicious Code

- Overview
- Attack Methodologies
- Investigative Responses



*U.S. Department of
Homeland Security*

United States
Secret Service

Malicious Code Attacks

- Viruses
- Trojans
- Worms
- Spyware
- Adware
- Rootkits



*U.S. Department of
Homeland Security*

United States
Secret Service

Investigative Responses

- Capture
- Preservation
- Warrants
- Reporting
- Education



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 7 – Denial of Service Attacks

- Overview
- Attack Methodologies
- Investigative Responses



*U.S. Department of
Homeland Security*

United States
Secret Service

Denial of Service

- Flooding target with more information than it can handle, causing system crash or reset
- Interfering with communications channel in such a way that others can't access system
- Starting so many processes on target system that available resources are used and system cannot respond to requests
- Changing access codes so that normal users can no longer access system



*U.S. Department of
Homeland Security*

United States
Secret Service

Distributed Denial of Service Attack

- When multiple systems attack target system
- Multiple systems usually compromised systems over which attacker has control



*U.S. Department of
Homeland Security*

United States
Secret Service

Investigative Responses

- Capture
- Preservation
- Warrants
- Reporting
- Education



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 8 – Extortion

- Overview
- Attack Methodologies
- Investigative Responses



*U.S. Department of
Homeland Security*

United States
Secret Service

Extortion on the Internet

- Direct threats
- Threats against tangible or non-tangible data
- Threats against a web entity
- Protection



*U.S. Department of
Homeland Security*

United States
Secret Service

Investigative Responses

- Capture
- Preservation
- Warrants
- Reporting
- Education



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 9 – Network Attacks

- Overview
- Attack Methodologies
- Investigative Responses



*U.S. Department of
Homeland Security*

United States
Secret Service

Attacking a Network

- Network routers
- Domain Name Servers
- Firewalls
- Intrusion Detection Systems
- Wireless networking equipment
- Access control systems



*U.S. Department of
Homeland Security*

United States
Secret Service

Investigative Responses

- Capture
- Preservation
- Warrants
- Reporting
- Education



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 10 – Terrorism

- Overview
- Attack Methodologies
- Investigative Responses



*U.S. Department of
Homeland Security*

United States
Secret Service

Terrorism

- Systematic creation of fear in group of people rather than individual
- Intimidation



*U.S. Department of
Homeland Security*

United States
Secret Service

Internet Use

- Psychological warfare
- Propaganda
- Fund-raising
- Message center for coordinating activities
- Launch network attacks
- Data mining



*U.S. Department of
Homeland Security*

United States
Secret Service

Internet Use

- Denial of Service attacks against enemies
- Site defacements of web sites counter to their cause
- Spam e-mail attacks against enemies
- Phishing attacks for banking information to help fund activities



*U.S. Department of
Homeland Security*

United States
Secret Service

Investigative Responses

- Capture
- Preservation
- Warrants
- Reporting
- Education



*U.S. Department of
Homeland Security*

United States
Secret Service

Module 9 – Phases of an Intrusion



*U.S. Department of
Homeland Security*

United States
Secret Service

You Will Learn . . .

- Defining and Intrusion
- Reconnaissance
- Network Attacks
- Entrenchment
- Infiltration and Extraction



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 1 – Defining and Intrusion

- Definition of an Intrusion
- Goals of an Intrusion
- Attacker Profiles
- Phases of an Intrusion



*U.S. Department of
Homeland Security*

United States
Secret Service

Intrusion

- Act of executing unauthorized actions against an information system and/or its resources
- Generally, considered to have taken place when someone gains unauthorized access to a computer
- When successful intrusion of single device occurs device is considered compromised
- Network intrusion is broader and includes compromise of multiple devices on single or multiple networks



*U.S. Department of
Homeland Security*

United States
Secret Service

Vulnerability

- A weakness in information system that could allow unauthorized actions to be taken against system



*U.S. Department of
Homeland Security*

United States
Secret Service

Exploit

- Tool used by an attacker to perform malicious attacks through vulnerabilities in system
- For example, error in an operating system that allows arbitrary code execution
- Program that attacker writes to perform attack against operating system error is exploit



*U.S. Department of
Homeland Security*

United States
Secret Service

Threats and Threat Agents

- Threats - Insider
 - Disgruntled employee
 - Uninformed employee
- Threat Agents
 - Contractors
 - Recruited or placed agent



*U.S. Department of
Homeland Security*

United States
Secret Service

Threats and Threat Agents

- Outsider
 - Hackers
 - Political activist “Hacktivist”
 - Information “brokers”
 - Foreign Governments or Corporations
- Natural disasters



*U.S. Department of
Homeland Security*

United States
Secret Service

Goals of an Intrusion

- *Denial-of-Server (DoS)* – Attack that makes computer resource unavailable
- *Unauthorized Access* – Act of gaining access to any computer resource without express permission of owner of resource
- *Inappropriate Usage* – Act of using computer resource in manner deemed inappropriate for resource



U.S. Department of
Homeland Security

United States
Secret Service

Goals of an Intrusion

- *Other* – Broad goals that may be difficult to categorize
 - Suspicious Activity – Any activity that does not conform to the normal prescribed activity
 - Malware – Software designed to infiltrate, monitor, or possibly damage a computer without the owner's consent



U.S. Department of
Homeland Security

United States
Secret Service

Intruder Types

- Many types of attackers and many reasons why networks and systems attacked
- Most intruders fit loosely into one of a few categories differentiated by skill, resources, and motivation
- Understanding basic intruder profiles and motivations may help identify other compromised systems



*U.S. Department of
Homeland Security*

United States
Secret Service

Intruder Types

- Advanced
- Intermediate
- Beginner



*U.S. Department of
Homeland Security*

United States
Secret Service

Advanced Attackers

- Skilled and motivated
- Generally exercise highest levels of caution and care
- Slow and precise
- Attempt to evade intrusion detection
- Attempt to hide signs of presence
- Attempt to mask source of attack



*U.S. Department of
Homeland Security*

United States
Secret Service

Advanced Attackers

- Piggy back on another attackers data stream
- Attempt to misdirect investigators by pointing to another source
- Program in one or more languages and will modify or create new exploit code/methods to support objective
- Working knowledge of common system network architectures
- Greatest ability to cause damage throughout network



*U.S. Department of
Homeland Security*

United States
Secret Service

Advanced Attackers

- Can be found in organized crime, terrorist organizations, foreign governments or next door
- Motivation varies, tends to match motivations of organization if associated
- Intellectual challenge is common motivation
- Sometimes categorized as Professional, State Sponsored, or Elite



*U.S. Department of
Homeland Security*

United States
Secret Service

Intermediate Attacker

- Attempt to follow same methodology as advanced group but do not possess necessary skills, knowledge or experience
- Moderate speed and precision
- May attempt to evade intrusion detection
- Attempt to remove signs of presence, but likely to miss something
- Attempt to mask source of attack



*U.S. Department of
Homeland Security*

United States
Secret Service

Intermediate Attacker

- May have programming skills and ability to perform minor modifications of exploit code to suit objectives
- Working knowledge of common system and network architectures
- Example, could be system administrator attempting to further his or her knowledge and abilities
- Other terms for intermediate attacker, Amateur and Enthusiast



*U.S. Department of
Homeland Security*

United States
Secret Service

Beginner Attacker

- User just getting into arena
- Learning, relies on success and failures of others to teach them basics
- Tendency to rely on other's code and scripts to do their work
- Do not have basic understanding of intrusion phases
- Usually fast and imprecise
- Does not usually attempt to evade intrusion detection, unless a function of tool they are using



*U.S. Department of
Homeland Security*

United States
Secret Service

Beginner Attacker

- No attempt to hide signs of presence, unless a function of tool
- May attempt to mask source of attack
- Normally cannot program well, if at all, no ability to modify exploit code to support objectives
- Motivations tend to be game-oriented, attacks for as little as bragging rights
- Other terms for beginner attacker are script kiddy, kiddiot, and packet monkey



*U.S. Department of
Homeland Security*

United States
Secret Service

Insiders

- Person authorized to use network or system due to membership in organization
- Often underestimated or overlooked as source because security focuses on protecting network perimeter from outside
- Virtually any disgruntled employee using valid account could take unauthorized actions against network
- Level of skill is highly varied, employee's motivations often include some form of sabotage or retribution



*U.S. Department of
Homeland Security*

United States
Secret Service

Phases of an Intrusion

- Not every intrusion will include all phases, specific actions will depend on objectives and abilities
- Reconnaissance – Gathering information about target
- Attack – Gathering, compiling, and launching exploits
- Entrenchment – Ensuring continued access to target system and hiding traces of access
- Extraction – Data theft or enabling channels for outbound attackers to new targets



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 2 – Reconnaissance

- Goals
- Strategies
- Techniques – General Web Browsing and Search
- Techniques – Public Records and Archives Search
- Techniques – Target Web Site Examination
- Techniques – Identifying Physical Attack Vectors
- Techniques – Live Host Identification
- Techniques – Identifying Available Ports/Protocols
- Techniques – Type and Version Identification
- Techniques – Vulnerability Scans



*U.S. Department of
Homeland Security*

United States
Secret Service

Reconnaissance Goals

- Target organization, including its main functions, staff members, assets, partner organizations, etc
- Target individuals, including names, functions, contact information, credentials, etc
- Target computers and networks, including addresses, functions, installed applications, operating systems, etc
- Any other information that may be beneficial



*U.S. Department of
Homeland Security*

United States
Secret Service

Direct versus Indirect

- Reconnaissance strategies can be defined as “direct” or “indirect”
- Direct techniques involve taking actions on or against information systems owned and/or operated by targeted individual or organization
- Actions may be observed and logged by target
- Indirect strategies do not involve actions on or against target information systems, will not be observed and logged by target



*U.S. Department of
Homeland Security*

United States
Secret Service

Reconnaissance Strategies

- General Web browsing and searching
- Public records searches
- Target Web site examination
- Identify physical attack vectors
- Live host identification
- Identification of open communication channels
- Operating system and application identification
- Operating system and application vulnerability scans



*U.S. Department of
Homeland Security*

United States
Secret Service

General Web Browsing and Search

- Valuable tool during information gathering phase, especially if used with information obtained by other means
- For example, Googling an employee's name produces home page with personal data or postings on newsgroups and discussion forums that yield sensitive company data
- Searches of online discussion forums, such as Usenet, may also reveal information about an organization's security weaknesses



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts

- Searching and browsing 3rd party Web sites typically do not generate any artifacts on information systems belonging to target organization or individual
- Will leave artifacts on network that hosts sites being browsed, most notably a record of URLs accessed during attacker's research



*U.S. Department of
Homeland Security*

United States
Secret Service

Public Records

- Domain Name Service (DNS)
- Whois
- Web site content archives
- Web site defacement archives
- Web server OS and Uptime
- Government business registration sites



*U.S. Department of
Homeland Security*

United States
Secret Service

DNS

- Used to maintain public record of domain names and corresponding IP addresses
- If you browse Microsoft.com, computer first asks DNS server how to find that domain name
- DNS will respond with IP addresses linked to Microsoft.com



*U.S. Department of
Homeland Security*

United States
Secret Service

DNS Records

- IP address of the Web server(s) that hosts the Web site for a particular domain name
- IP address of the e-mail server(s) that hosts e-mail for a particular domain name
- IP addresses of the DNS servers that are authoritative for a domain name
- Host/domain names associated with an IP address



*U.S. Department of
Homeland Security*

United States
Secret Service

Whois Records

- Several Regional Internet Registries (RIRs) responsible for leasing IP addresses to ISPs and other large organizations
- “Whois” is Internet utility that queries RIR database for public information
- Range of IP addresses assigned to an organization
- Geographical address used when organization registered domain
- Names or handles, phone numbers, and e-mail addresses of points of contact (POCs) for an organization



*U.S. Department of
Homeland Security*

United States
Secret Service

Web site Content Archives

- Wayback Machine (<http://www.archive.org>) provides archival storage for Web pages no longer available through original provider
- Wayback Machine offers ability to check for previous, less security-conscious versions of organization's site



*U.S. Department of
Homeland Security*

United States
Secret Service

Defacement Archives

- Defacement archival sites provide information, archives, and statistics regarding Web defacements
- Example is Zone-H (<http://www.zone-h.com>)
- Attackers can use Zone-h to learn if target has been defaced previously
- Record of defacement and listing of operating system and Web server in use at time of compromise may be available



*U.S. Department of
Homeland Security*

United States
Secret Service

Web Server OS and Uptime Archives

- Netcraft (<http://news.netcraft.com>) site provides network and server-specific search functionality
- Enter domain name, Netcraft will determine operating system and uptime of server to which domain name points
- Netcraft attempts to discover type of Web server application running and will provide record of results for previous attempts to gather information



*U.S. Department of
Homeland Security*

United States
Secret Service

Government Business Registration Sites

- For tax and liability purposes, federal and most state governments require businesses submit several forms
- Forms often public record and searchable on Internet for information about potential targets
- For example, the U.S. Securities and Exchange Commission's EDGAR (Electronic Data Gathering, Analysis, and Retrieval) system



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts

- Searching third-party archive and public record sites typically will not generate artifacts on systems belonging to target organization or individual
- Will leave artifacts on network that hosts sites being browsed, most notably record of URLs accessed during attacker's research
- Possible that queries made against third-party DNS server will be forwarded to DNS server owned or operated by target organization



*U.S. Department of
Homeland Security*

United States
Secret Service

Target Web Site Examination

- Target organization Web sites can serve an attacker as either source of general information or as point of entry into network
- During recon, the following tactics may be used when reviewing a site:
 - Manual browsing
 - Automated crawling
 - URI prediction/guessing
 - Source code review



*U.S. Department of
Homeland Security*

United States
Secret Service

Manual Browsing

- Manually browsing target Web site is legitimate method for gathering intelligence about site and organization running site
- Disadvantage, it is a direct technique, will leave traces on target system and network
- Can pattern can mimic legitimate user or be obfuscated by use of various proxies or routing techniques
- Browsing could also be routed through another previously compromised box



*U.S. Department of
Homeland Security*

United States
Secret Service

Automated Crawling

- Web crawlers (AKA Robots or Spiders) can be used to automatically browse site and follow all available links
- Results of Web page download from each link, saved for later review.
- Technique very obvious to anyone that reads logs of target Web server or any associated reverse proxies



*U.S. Department of
Homeland Security*

United States
Secret Service

URI Prediction

- Not all pages at Web site accessible via link
- Pages not directly advertised on site or linked sometimes found by guessing at naming convention used by site designer
- Guessing naming conventions can lead to discovery of additional pages containing valuable data
- Guessing resources can lead to error logs on server
- Can be generic errors or in the case of a restricted folder, security-related errors



*U.S. Department of
Homeland Security*

United States
Secret Service

Source Code Review

- Other than server side scripts, all HTML/XML markup language and client-side scripts, sent to Web browser that requests associated page
- Code can be reviewed for information disclosure (in programmer comments for example), as well as for weaknesses in code itself



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts

- Any record of URL requests from suspicious IP addresses or IP ranges in logs of Web server or associated Web proxies
- Logs that show broad, systematic pattern of URL requests, characteristic of site being crawled
- Logs that show failed URL access attempts that list non-existent files close in name to actual existing files
- IDS alerts referencing Web crawling or other abnormal URL access patterns



*U.S. Department of
Homeland Security*

United States
Secret Service

Attack Vectors

- A pathway through which an attack may be launched
- Most common attack vector is via Internet, a mixture of physical mediums
- There are times when specific vectors will be useful or even required, such as when target cannot be reached via Internet



*U.S. Department of
Homeland Security*

United States
Secret Service

Attack Vectors

- POTS (Plain Old Telephone System)
- Wireless
- Direct physical access to the device
- Mixed (any route across the Internet)



*U.S. Department of
Homeland Security*

United States
Secret Service

Identifying POTS Vectors

- War-dialing is identifying computers listening for remote connections on a POTS line, if response received, computer is listening, further attack actions may be taken
- Growing less viable as more systems use dedicated Internet connections rather than dial-up modems



*U.S. Department of
Homeland Security*

United States
Secret Service

Identifying Wireless Vectors

- Attackers can use computer with 802.11 network interface to listen for frames transmitted from 802.11 compliant wireless networks
- Different 802.11 specifications, attacker would have to ensure that attack wireless NIC(s) supported all necessary versions
- Other wireless specifications not typically viable vector, but cellular access to information systems becoming more prevalent and Bluetooth can be used in close range situations



*U.S. Department of
Homeland Security*

United States
Secret Service

Identifying Physical Vectors

- An attacker could obtain direct physical access to a target device through unauthorized access to building/room
- If target device is owned by organization to which attacker is employed, physical access may already be available



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts

- Call records that show incoming calls to phone number with modem attached
- Standard physical security violations or suspicious activity (e.g. unknown persons in building, tripped alarms, broken locks, etc.)
- Console logins recorded in system logs during times when building empty, or when owner of user account not present
- 802.11 frames from an unknown source
- Presence of physical wiretap devices on a cable or device



*U.S. Department of
Homeland Security*

United States
Secret Service

Live Host Identification

- The process of finding target hosts and verifying they are online responding to communication requests
- Can be done through several methods:
 - ICMP probes/sweeps
 - TCP/UDP probes/sweeps
 - Network monitoring



*U.S. Department of
Homeland Security*

United States
Secret Service

ICMP Probes/Sweeps

- ICMP protocol used primarily for network troubleshooting, and commonly to test hosts to see if they are online
- ICMP “Echo Request” packet used to sweep multiple IP addresses to elicit “echo response” packet from available hosts
- Also called “ping sweep”
- To pass through firewalls that block ICMP Echo Requests, other ICMP packet types may be used to elicit response from target host



*U.S. Department of
Homeland Security*

United States
Secret Service

TCP/UDP Sweeps

- Modern networks sometimes block ICMP at external perimeter defenses (firewalls and routers)
- TCP and UDP packets can be sent instead in attempt to circumvent this barrier



*U.S. Department of
Homeland Security*

United States
Secret Service

Network Monitoring

- Passively monitoring network from compromised system can identify other hosts instead network
- Amount of traffic collected and number of hosts identified will depend greatly upon sniffer placement within logical network architecture



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts

- IDS alerts referencing broad scans or sweeps
- Firewall logs that show blocked packets attempting to reach a large number of hosts in a short period of time
- Firewall logs that show traffic blocked based upon abnormal protocol options (unusual ICMP types, TCP ACK packets existing outside of a session, etc.)



*U.S. Department of
Homeland Security*

United States
Secret Service

Ports/Protocols

- Once physical vector identified, and target verified as being online, attacker may choose to enumerate methods by which target computer is willing to communicate
- Communication methods include:
 - Accepted network and transport protocols (ICMP, TCP, UDP)
 - Accepted application protocols (HTTP, FTP, SMTP, etc.)
 - Accepted TCP/UDP port numbers



*U.S. Department of
Homeland Security*

United States
Secret Service

Identifying TCP/UDP Port Numbers

- Also called “Port Scanning,” connection attempts can be sent to TCP and UDP ports to determine if application is listening
- Scanner may attempt to initiate TCP session to multiple ports
- Response to request with a TCP syn/ack packet, indicates there is application or OS service listening on port



*U.S. Department of
Homeland Security*

United States
Secret Service

Identifying TCP/UDP Port Numbers

- Scanner sends packets to UDP ports to test if ports are open
- Since UDP is connectionless, packets either empty, or contain data that not valid for protocol normally used with port
- If port is open, the application listening on port will respond,
- If port not open, ICMP Destination Unreachable message sent



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts

- IDS alerts referencing port/protocol scans.
- Firewall logs showing blocked attempts to access large number of ports, in close sequence, on single host, in short time
- TCP session initiated to IP address, immediately terminated, not followed by additional communication, observable in sniffer log
- TCP session only half set up then abandoned, potentially observable in sniffer log



*U.S. Department of
Homeland Security*

United States
Secret Service

Type and Version Identification

- Once open communication channel to device established, attacker may need to know type and version of listening application and/or operating system
- Attack methods are highly dependant upon target versions and patch levels
- Common methods for identifying this information include:
 - Banner grabbing
 - Packet printing



*U.S. Department of
Homeland Security*

United States
Secret Service

Banner Grabbing

- Process of connecting to commonly available services that provide type and version information in greeting messages



*U.S. Department of
Homeland Security*

United States
Secret Service

Packet Printing

- TCP/IP stack is part of operating system that controls TCP/IP network communication
- Implementation of stack differs on every operating system, produces minor variances in operating system's response to certain requests
- Scanning tools that perform packet printing (or fingerprinting) check for variances on target host to identify operating system



*U.S. Department of
Homeland Security*

United States
Secret Service

Attributes Used for Packet Printing

- ICMP Error Messages
- TCP Sequence Numbers
- TCP Options
- TCP Timestamps
- TCP Retransmissions Timeouts
- Fragmentation Handling
- IPID Values



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts

- IDS alerts referencing scans
- Errors in logs of scanned application or service referencing communication problems or incomplete connection attempts



*U.S. Department of
Homeland Security*

United States
Secret Service

Targets for Vulnerability Scans

- Web servers and FTP servers
- E-mail servers
- File and database servers
- Directory service servers
- RPC
- Print services
- Simple services



*U.S. Department of
Homeland Security*

United States
Secret Service

Vulnerability Scan Techniques

- Presence of known vulnerable application component files
- Ability to traverse into normally non-accessible directories on host operating system
- Ability to access unauthorized files
- Ability to execute unauthorized code



*U.S. Department of
Homeland Security*

United States
Secret Service

Vulnerability Scan Techniques

- Ability to make unauthorized calls to backend application or database servers
- Ability to route unauthorized data, such as spam or another probe, through the server
- Ability to trigger backchannel communication, a communication session originating from target to hacker



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts

- IDS alerts referencing a possible vulnerability scan
- IDS alerts referencing any attack (Some vulnerability scans launch partial attacks to determine if they're possible, this may trigger an IDS)
- Any extremely large volume of traffic that is widely varied, characteristic of comprehensive (multi-protocol), blatant vulnerability scan
- Any other activity characteristic of any attack



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 3 – Network Attacks

- Goals
- Strategic Categories
- Strategies – Authentication Attacks
- Techniques – Factor Guessing/Cracking
- Techniques – Credential Recover/Reset
- Techniques – Credential Injection
- Techniques – Credential Theft



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 3 – Network Attacks, continued

- Strategies – Unexpected Input
- Techniques – Excessive Input
- Techniques – Excessive Input / Buffer Overflows
- Techniques – Unexpected Input Content / XSS Attacks



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 3 – Network Attacks, continued

- Techniques – Unexpected Input Content / XSS Attacks
- Techniques – Unexpected Input Content / Command Injection
- Techniques – Unexpected Input Timing
- Techniques – Unexpected Input Timing / Temp File Attacks
- Techniques – Unexpected Input Timing / Request-Response Latency Attacks
- Techniques – Unexpected Input Timing / Boot Process Attacks



*U.S. Department of
Homeland Security*

United States
Secret Service

Entrenchment Goals

- Unauthorized Access: Obtaining access to resource (system, network, data, etc.) that is illegal, against policy, or otherwise unauthorized by organization/individual owning resource
- Access Privilege: Obtaining ability to manipulate resource (change, delete, deactivate, etc.) to extent not authorized by organization/individual owning resource
- Denial of Service: Preventing resource from being available to fulfill purpose either temporarily or permanently



*U.S. Department of
Homeland Security*

United States
Secret Service

Entrenchment Strategic Categories

- Authentication Attacks: Attacks against authentication mechanism for purpose of obtaining credentials to system or network
- Unexpected Input: Supplying input in way that will cause application or operating system to behave in unauthorized fashion, either to gain unauthorized access or disrupt functionality of target system



*U.S. Department of
Homeland Security*

United States
Secret Service

Authentication Attack Strategies

- Factor guessing/cracking: Attempting to determine factors (passwords for example) to allow authentication to system
- Credential recovery/reset: Taking actions to cause system or administrator to send set of credentials to attacker
- Credential injection: Creation of new credentials that will allow authentication into target system
- Credential theft: Theft of credentials either through inadvertent disclosure or methods such as sniffing network traffic



*U.S. Department of
Homeland Security*

United States
Secret Service

Authentication and Authorization

- Authentication attacks focus on obtaining credentials for specific individual or account, or being authenticated as person or account without credentials
- What attacker can accomplish will depend on what compromised/unauthorized account is allowed
- If attacker requires more authority on system or network, he/she will use another authentication attack, or different attack strategy



*U.S. Department of
Homeland Security*

United States
Secret Service

Authentication Factors

- “Something you know”: Usernames, passwords, pass-phrases, answers to secret questions, etc
- “Something you have”: USB tokens, smart cards, RFID tokens, cookies, encryption keys, etc
- “Something you are”: Retinal patterns, thumbprints, DNA, etc



*U.S. Department of
Homeland Security*

United States
Secret Service

Guessing/Cracking

- Attacker generate set of values that represent possible legitimate authentication factors
- Attacker tests values against authentication system or stolen set of password hashes to determine which ones are correct, if any



*U.S. Department of
Homeland Security*

United States
Secret Service

Value Generation

- Brute Force: Guessing every possible value for credential using any combination of acceptable characters
- Dictionary: Using only words from a dictionary to generate a list of potential values, some attacks allow for small variances such as common misspellings in the list of potential values
- Hybrid: Using any combination of brute force and dictionary mehtods



*U.S. Department of
Homeland Security*

United States
Secret Service

Value Generation

- Pattern Recognition: For server/administrator assigned factors that follow a pattern, an attacker could use the pattern to guess the values of other valid factors
- Pre-generated Hashes: When authentication factor is a hash value of another piece of data, such as hash of password, list of all possible hashes for a set of values can be pre-calculated, term “rainbow table” is used to refer to some types of pre-generated hash sets



*U.S. Department of
Homeland Security*

United States
Secret Service

Value Testing

- Manually typing values in one at a time
- Using an automated tool such as THC Hydra to pass test values to authentication system
- Using hashes calculated against values in set of data and comparing to hashes stolen from authentication system or used by authentication system



*U.S. Department of
Homeland Security*

United States
Secret Service

Value Testing and Session Length

- When a session is underway and individual or application is authenticated, that session will sometimes last for specific amount of time
- If credentials successfully guessed/cracked, may only be good for length of session in progress
- Likely the case when factor is temporary token, such as a cookie



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts

- Large numbers of failed authentication attempts for single account seen in logs of authentication system
- Failed authentication attempts for one or more non-existent user account names
- Failed authentication attempts that show series of passwords that match pattern indicative of attack
- IDS logs referencing password or authentication attack



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts

- User accounts locked out due to high number of failures
- List of passwords or password hashes found in text file in abnormal location
- The presence of password/hash dumping utilities such as pwdump (pwdump.dll)
- Authentication attempts (successful or failed) at abnormal times, or for which authorized user of account does not recall



*U.S. Department of
Homeland Security*

United States
Secret Service

Credential Recovery and Reset

- Users lose credentials (authentication factors), forget password, lose tokens and sometimes can't remember their user names
- Most authentication systems include mechanism for resetting a user's credentials to a new value, or recovering copy of lost credentials



*U.S. Department of
Homeland Security*

United States
Secret Service

Recovery/Reset Mechanisms

- Password reset links on Web sites
- Help desk staff (available by phone or in person) that reset or unlock an account
- Operating system and directory user account management interfaces that allow account with sufficient privilege to reset credentials to other accounts



*U.S. Department of
Homeland Security*

United States
Secret Service

Credential Recovery/Reset Attack Techniques

- Requesting a password reset, and capturing password from network
- Registering a domain name previously belonging to another person, recreating a previously existing e-mail address at domain name, and using e-mail address as an authentication factor and recipient for reset credentials transmissions
- Directly requesting an individual's credentials, while using personal information about that individual



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts

- Successful authentication attempts for account believed to be no longer in use
- Password resets for an account that was believed to be no longer in use
- Password resets for which the legitimate user of the account claims to not be responsible



*U.S. Department of
Homeland Security*

United States
Secret Service

Credential Injection

- Calling a help desk and requesting creation of an account
- Using an online mechanism to request an account
 - Can be done to gain initial access to information on Web sites that provide information
 - Some Web sites might require user validate identify for registration, using some type of personal information
 - Others allow input of whatever information user chooses to provide
- Directly creating user accounts using administrative utility



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts

- Existence of user account in account repository for which there is no legitimate authorized user
- Existence of user account in account repository that does not match account naming convention for organization
- Recorded logins of account for which there is no legitimate authorized user
- Log entries referencing account creation



*U.S. Department of
Homeland Security*

United States
Secret Service

Credential Theft

- Capturing credentials as transmitted across network
 - Requires attacker have control or be present on one of network mediums through which credentials sent
- Tricking an individual into revealing credentials
 - Social Engineering
- Stolen physical tokens such as ID cards and USB tokens



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts

- Reports of theft of physical credentials or of disclosure of credentials to someone believed authorized to make request
- Successful authentication requests at abnormal times, or for which authorized user of account does not recall
- Existence of e-mails in e-mail repository or logged by proxy that include requests for credentials, or links to Web pages where such requests are made



*U.S. Department of
Homeland Security*

United States
Secret Service

Unexpected Input Strategies

- Excessive Input: Sending more input than system or application was expecting, or is able to handle
- Unexpected Input Content: Sending input content that system or application will process incorrectly due to inability to recognize and/or properly control input type
- Unexpected Input Timing: Sending input at times that system, application or communication session is temporarily vulnerable to interference



*U.S. Department of
Homeland Security*

United States
Secret Service

Excessive Input

- Take advantage of a lack of input validation
- Basic attack method to supply an excessive amount of input to an application, operating system, or network
- Effect could be to crash target or break a control system and allow attacker to perform additional unauthorized actions
- Buffer Overflow Attacks
- Flooding



*U.S. Department of
Homeland Security*

United States
Secret Service

Input Size Validation

- Properly coded applications should verify user-supplied input is of proper size, If not, truncate input or produce error message and/or stop the process
- Network devices should terminate or block all communication from hosts supplying excessive number of packets or service requests



*U.S. Department of
Homeland Security*

United States
Secret Service

Excessive Input/Buffer Overflow

- *Buffer* is temporary storage area, usually in RAM, allocated for manipulation of data within a process
- For instance, when logging into e-mail server, 32-character space for username
- Limitation is established in code of e-mail server application and controls how much input will be accepted from user



U.S. Department of
Homeland Security

United States
Secret Service

Buffer Overflow Attack

- Purposely sends entry too large for buffer
- Sends in such a way that portion of entry is written to target computer where program instruction code stored
- Attacker uses method to intentionally cause execution of code
- Result of code execution could be anything, but will often be denial-of-service, command terminal session sent back to attacker's computer or injection of DLL or other program code



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts

- Unexplained errors in the log files for application or service attacked
- Intrusion detection system alerts indicating a buffer overflow
- Sniffer logs show large blocks of repetitive data, such as 0x90 or other hex values
- Sniffer logs show blocks of data that do not conform to normal rules for network protocol used
- IDS alerts or sniffer logs showing common post-attack events such as reverse shells, DLL transfer, OS commands, etc.



*U.S. Department of
Homeland Security*

United States
Secret Service

Cross-Site Scripting (XSS)

- Cross-site scripting occurs when attacker supplies script executed by another system's Web browser or in another browser window accessing a different site



*U.S. Department of
Homeland Security*

United States
Secret Service

Cross-Site Scripting (XSS)

- Attacker posts script to website that permanently stores script
- Serves it to other systems when they request the web page to which it was posted
- Allows attacker to run code in another person's browser, “persistent” or “stored” XSS attacks



*U.S. Department of
Homeland Security*

United States
Secret Service

Cross-Site Scripting (XSS)

- Attacker will embed script in URL
- If loaded by another user, will cause Web server to supply malicious code to requesting browser to be executed in context of requested page
- Called “non-persistent” or “reflected” XSS attacks, rely on user or browser to load the URL



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts of XSS

- IDS alerts referencing an XSS attack
- URLs containing scripting as seen in Web server and proxy server logs, or in Web browser history
- Web pages containing embedded scripting, as seen in proxy server logs where proxy records full page
- Unusual character encodings in URLs as seen in Web server or proxy server logs, or in Web browser histories



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 4 - Entrenchment

- Goals
- StrategiesTechniques – Log
- CleaningTechniques – Automatic
- ExecutionTechniques – Hooking
- Techniques – File Type Manipulation
- Techniques – Naming Conventions and Placement
- Techniques – Remote Connectivity
- Techniques – File System Date/Time Stamp Manipulation



*U.S. Department of
Homeland Security*

United States
Secret Service

Entrenchment Goals

- Attack Pivot Point: Attacker requires continued control of system to use as pivot point from which to attack other systems and networks
- Data Theft: Attacker requires continued control of system to perform data mining operations on system and any local storage media.
- General Control: Attacker wants to maintain control of system as asset for various other uses



*U.S. Department of
Homeland Security*

United States
Secret Service

Entrenchment Goal Attributes

- Entrenchment requires attacker retain some ability to remotely control or manipulate target,
- Method of control must remain undetected



*U.S. Department of
Homeland Security*

United States
Secret Service

Entrenchment Strategies

- Log Cleaning: Removing records of unauthorized activities to hide presence
- Automatic Execution: Adding configuration changes that will cause unauthorized programs to be started when host OS boots, or restarts
- Naming Conventions and Placement: Naming unauthorized files, processes and configuration changes in way that they appear legitimate or otherwise benign



*U.S. Department of
Homeland Security*

United States
Secret Service

Entrenchment Strategies

- File Type Manipulation: Changing attributes which identify a file's type, such as signature and extension
- Hooking: Intercepting calls to operating system so as to interfere with data returned
- Remote Connectivity: Maintaining one or more channels through which compromised system can be remotely controlled



*U.S. Department of
Homeland Security*

United States
Secret Service

Entrenchment Unauthorized Code

- Entrenchment activities typically involve installation of unauthorized code
- This code will serve to perform one or more of functions identified on previous slides
- Common types include backdoors, rootkits and trojans



*U.S. Department of
Homeland Security*

United States
Secret Service

Log Cleaning

- Attacker must remove records of unauthorized activity
- Common record of unauthorized activity is a log entry
- Log cleaning is process of deleting individual log entries, or clearing entire log files to achieve goal
- Can be done manually, with specific log cleaner malware, or with a general-purpose rootkit



*U.S. Department of
Homeland Security*

United States
Secret Service

Log Cleaning – Record Deletion

- Removing individual records easy with text logs
- Attacker opens log in a text editor, deletes associated lines and saves file
- Proprietary log formats are much more difficult to handle
- Attacker (or tools) must understand format of log, and be able to identify beginning and end of each entry
- Log viewers that correspond to proprietary logs do not typically include function for removing individual entry



*U.S. Department of
Homeland Security*

United States
Secret Service

Log Cleaning – Log Clearing

- Alternative to deleting individual records, clear an entire log
- Done in situations where attacker is in hurry or does not have mechanism for deleting individual records
- Downside of log clearing is that it is quite noticeable
- Attacker may clear log when not concerned with hiding intrusion but more with removing information used to trace attack back to source (not characteristic of entrenchment)



*U.S. Department of
Homeland Security*

United States
Secret Service

Log Cleaning – File Deletion

- Attacker may choose to delete entire log file In lieu of record deletion or log clearing
- Least desirable of log cleaning methods as deletion of log file is most noticeable and may cause system errors or crashes
- More likely when dealing with more obscure log files not as likely to be noticed



*U.S. Department of
Homeland Security*

United States
Secret Service

Log Cleaning – Possible Artifacts

- File system date/time stamps changed during log cleaning
- Log files that have had specific entries removed may have abnormal time gaps between remaining entries
- Empty or completely missing log files
- Log entry indicating log was cleared
- Existence of malicious code on system that includes log cleaning as one of its functions



*U.S. Department of
Homeland Security*

United States
Secret Service

Automatically Starting Malware

- Common for malicious code to be installed such that it will start automatically when Windows boots
- Main mechanism for accomplishing this is by adding Registry key that will start executable file as new process or load library into another process
- Common methods include creating “Run” keys for executables, installing new service, or trojanize legitimate service by changing ServiceDLL key to load malicious DLL



*U.S. Department of
Homeland Security*

United States
Secret Service

Automatic Execution Directories

- C:\Documents and Settings\All Users\Start Menu\Programs\Startup
- C:\Documents and Settings\<username>\Start Menu\Programs\Startup
- C:\Windows\Tasks



*U.S. Department of
Homeland Security*

United States
Secret Service

Job Scheduling

- Most operating systems include mechanism for scheduling executions to occur with various triggers, usually date/time
- For Microsoft operating systems the Windows Task Scheduler
- For Linux/Unix derivatives the “cron” daemon



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts

- Existence of Registry entries that load unauthorized executables or libraries
- Unauthorized executables in auto-start directories
- Unauthorized executables specified in an INI file
- Existence of “.job” files on Windows
- Entries in “crontab” file in Linux/Unix derivatives
- Malicious code found on system which adds automatic start configurations when executed



*U.S. Department of
Homeland Security*

United States
Secret Service

Hooking

- Process of intercepting calls from one program to another so as to interfere with any data exchanged
- Can be used to hide data such as processes, files and specific file contents



*U.S. Department of
Homeland Security*

United States
Secret Service

The OS API

- API (Application Programming Interface) defined so programs can be written that will run on and interface with OS
- Functions that use API:
 - Directory listings
 - File copy and move operations
 - File editing operations
 - Network sending and receiving
 - Process and thread starting, stopping and enumeration



*U.S. Department of
Homeland Security*

United States
Secret Service

The OS API

- For instance, when Windows Explorer used to view contents of a directory, it is done via a standard API call from explorer.exe to Windows OS DLL file
- Operations are common during every day usage of OS
- During entrenchment, same API calls used to find malicious code
- Important to attacker to prevent calls from revealing signs of malware presence



*U.S. Department of
Homeland Security*

United States
Secret Service

OS API Hooking

- Rootkits can be used to hook API calls, intercepting them at various points
- Sensitive values can be edited out of any returned values



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts of API Hooking

- Hash values of OS files that have been hooked through direct modification will be modified
- Modified hash values for files indicates potential presence of API hooks in memory
- Technique is used by some rootkit detection programs such as Rootkit Revealer
- Discovery of API hooks during analysis of malicious code files found on compromised system



*U.S. Department of
Homeland Security*

United States
Secret Service

File Type Manipulation

- Attributes that define a file's type can be manipulated to hide file from general searches and from some specific forensic analysis
- Changing file extension to make file appear a different file type
- Changing file signature to make file appear as a different file



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts

- File signatures that do not match extension, or vice versa
- Files that have a matching signature and extension, but which cannot be read by appropriate application



*U.S. Department of
Homeland Security*

United States
Secret Service

Naming Conventions Strategies

- Giving files/processes the same name as a legitimate file or process
- Giving files/processes a name that is slightly modified from name of a legitimate file or process
- Assigning a name that appears similar to the names of other files
- Use of special characters within names that will cause name to blend in with other files, or will cause name to not be rendered in certain interfaces



*U.S. Department of
Homeland Security*

United States
Secret Service

Placement Strategies

- Placing unauthorized files in a directory where average user unlikely to look
- Placing unauthorized files named a certain way into a directory with other files with similar names
- Using normal directory names, but in wrong location, temp directory often used
- Storing files or file fragments in disk space not currently in use
- Fragmenting file and inserting it into another file in small amounts



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts

- Files, Registry keys and processes misspelled or in wrong location
- Files that do not have appropriate hash value or file signature
- Process running in more than one instance when not typical, or when process is child of itself
- Presence of programs on system used for file hiding
- File names and directory locations discovered during analysis of malicious code



*U.S. Department of
Homeland Security*

United States
Secret Service

Remote Connectivity

- For extended operations intruder will require dependable access to compromised systems
- Could be legitimate channel that attacker accesses with stolen credentials, or new channel created by attacker



*U.S. Department of
Homeland Security*

United States
Secret Service

Subverting Legitimate Communication Channels

- SMB/CIFS & DCE/RPC
 - Windows file sharing and remote procedure protocols
 - used to move data to and from, or even configure a remote system
 - Requires attacker has credentials to system
 - most useful for manipulating a system from another device within same network



*U.S. Department of
Homeland Security*

United States
Secret Service

Subverting Legitimate Communication Channels

- Remote administration applications
 - Terminal Services, VNC and Remote Desktop
 - Allow someone to open a graphical interface to another system
 - Attacker can authenticate to these pre-existing applications with stolen credentials
 - Other applications such as SSH and telnet used to administer a system through a command line interface



*U.S. Department of
Homeland Security*

United States
Secret Service

Subverting Legitimate Communication Channels

- VPN tunnels:
 - Attacker can utilize tunnels that already exist to or from compromised system to jump to other devices and/or networks



*U.S. Department of
Homeland Security*

United States
Secret Service

Remote Backdoors

- A non-legitimate method for listening for remote connections from attacker to compromised system
- Typically accomplished by starting process that listens for remote connection attempts
- Might be normal TCP connection attempt, or may involve series of packets sent to specific ports in specific order which will cause full listening socket to open (called “port knocking”)



*U.S. Department of
Homeland Security*

United States
Secret Service

Outbound Initiated Channels

- Compromised system may sit behind firewall, prevents inbound remote connection attempts
- Alternative to process listening for inbound connection attempts, malicious code package configured to initiate outbound communication
- Connections, called “Reverse Channels,” frequently successful due to fact that firewall egress rules are typically less stringent than ingress rules



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts: Legitimate Channel Usage

- Unusual login times for otherwise authorized account.
- Logins for authorized account that user of account did not initiate
- Authentication or subsequent activity that occurs too fast for human to be manually directing activity
- Existence of malicious code on compromised system that includes functions for connecting to remote administration applications such as SSH or VNC



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts: Backdoors

- Abnormal ports open on a system
- Suspicious processes attached to a listening port
- Inbound connection attempts to workstations
- Abnormal patterns of inbound packets or connection attempts
- Existence of malicious code on compromised system found to start listening service when executed



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts: Outbound Channels

- DNS queries for known-bad domain names or DNS hosts
- Outbound connection attempts to known-bad or suspicious IP addresses or IP ranges
- Outbound connection attempts occurring over abnormal ports
- Outbound connection attempts which exhibit abnormal content
- Existence of malicious code on compromised system found to beacon to domain name or IP address when executed



*U.S. Department of
Homeland Security*

United States
Secret Service

File System Date/Time Stamp Manipulation

- Attacker may attempt to hide unauthorized activity by changing associated date/time stamps
- Attempt to make it appear as if activity is unrelated



*U.S. Department of
Homeland Security*

United States
Secret Service

Possible Artifacts

- Date/time stamps for malicious code executables or DLLs that match date/time stamps on files created much earlier than other related activity
- Date/time stamps for suspicious Registry keys that are set much earlier than other related activity
- Existence of malicious code on system found to modify date/time stamps on files or Registry keys when executed



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 5 – Infiltration and Extraction

- Sniffers
- Trust Relationships
- Data Extraction



*U.S. Department of
Homeland Security*

United States
Secret Service

Sniffers

- A program used to monitor or capture network traffic
- Collected data usually stored on compromised system in hidden file
- Often run as disguised processes on systems as:
 - Trojanized device drives
 - Renamed programs configured to start at boot
 - Trojanized applications



*U.S. Department of
Homeland Security*

United States
Secret Service

Trust Relationships

- Mechanism whereby users logged on and authenticated to one server can access resources on another without need to re-authenticate
- If server A trusts users logged into server B, server A has established a one-way trust
- If server A trusts server B, and server B trusts server A, they have established a two-way or absolute trust
- If A and B have a two-way trust and B also trusts C, C can access A through a pass through or transitive trust



*U.S. Department of
Homeland Security*

United States
Secret Service

Trust Relationships

- Server A ←----- Server B (One way trust)
- Server A ←-----→ Server B (Two-way or absolute trust)
- Server A ←-----→ Server B ←-----Server C (Transitive trust)



*U.S. Department of
Homeland Security*

United States
Secret Service

Trust Relationship Exploitation

- Compromising a trusted system, domain or server
- Using or exploiting the LDAP service
- Forging or spoofing authentication credentials
- Spoofing source information
- Piggybacking off an already trusted system
- Hijacking a session from a trusted system



*U.S. Department of
Homeland Security*

United States
Secret Service

Data Extraction

- Process of obtaining data off compromised system
- To avoid detection, desired data is filtered for relevancy and sent in way that will not overload system or trigger IDS
- Embedding data deep into packets often allows extraction of data without detection
- Hacker may schedule job to send data during time when network traffic is heavy in attempt to avoid detection by using network traffic volume



*U.S. Department of
Homeland Security*

United States
Secret Service

Data Extraction Methods

- E-mail
- Masked as services like HTTP, DNS or ARP
- Backdoor connections
- Services run on a regular basis
- Ftp or telnet login by attacker
- A print job run to a remote location or file



*U.S. Department of
Homeland Security*

United States
Secret Service



*U.S. Department of
Homeland Security*

United States
Secret Service

Module 10 – Report Writing



*U.S. Department of
Homeland Security*

United States
Secret Service

You Will Learn . . .

- General Report Writing Techniques
- Specific Report Templates
- Interviewing Techniques



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 1 – General Report Writing Techniques

- Examiner Notes
- Forensic Reporting
- Title Page
- Items Analyzed
- Relevant Software
- Glossary
- Details of Findings
- Items Provided
- Hyperlinking



*U.S. Department of
Homeland Security*

United States
Secret Service

Forensic Report

- Culmination of time intensive, painstaking work
- Should reflect time, effort, professionalism put forth to acquire information presented
- Should be organized, clear, concise, free of grammatical and punctuation errors
- Consider report reflection of yourself, your skills, attention to detail, experience and work ethic



*U.S. Department of
Homeland Security*

United States
Secret Service

Examiner Notes

- Documentation created during investigative and analysis processes, provides basis for examiner to report results of case
- Written notes and documentation created during investigation should be preserved and may be discoverable
- Examiner notes taken during execution of forensic examination, along with final report of findings are foundation on which many digital media-related cases are built



*U.S. Department of
Homeland Security*

United States
Secret Service

Note Taking

- Essential part of a forensic examination
- Assists in creation of document that will provide record of procedures and processes performed
- Examination notes should present clear timeline of actions taken and results of actions
- Properly recorded notes provide repeatable roadmap of examination
- Another examiner should be able follow notes to reproduce same results obtained in original exam



*U.S. Department of
Homeland Security*

United States
Secret Service

Note Taking

- Number, date, and initial all note pages using [page #] of [total # of pages] numbering schema to account for all pages
- Not uncommon for extensive periods of time to pass between time of examination and prosecutorial action
- Thorough note taking helps ensure accurate testimony as to actions taken during examination
- Follow rule, “If it wasn’t documented, it didn’t happen”



*U.S. Department of
Homeland Security*

United States
Secret Service

Forensic Report

- Provide details about purpose for forensic analysis
- Describe physical and/or logical evidence analyzed
- Define related programs, terms and their relevance



*U.S. Department of
Homeland Security*

United States
Secret Service

Forensic Report

- Clearly identify persons related to examination including yourself, requestor, suspects, other pertinent individuals
- Address relevant evidence found during examination
- Clearly, concisely explain items of evidentiary value found on suspect media during analysis
- Identify location and relevance of items of evidentiary value as relating to reason for analysis and/or investigation



*U.S. Department of
Homeland Security*

United States
Secret Service

Forensic Report

- Should define all technical terms using common language that non-technical investigators and prosecutors can understand
- Should always contain information listed on following slide, headings may vary from organization to organization



*U.S. Department of
Homeland Security*

United States
Secret Service

Report Contents

- Report heading
- Support requested, reason or purpose for analysis
- Summary of findings
- Digital media analyzed
- Analysis/Suspect software listings
- Glossary of technical terms
- Details of findings
- Items provided



*U.S. Department of
Homeland Security*

United States
Secret Service

Title Page

- Report Header
- Support Requested
- Current Case Status
- Summary of Findings
- See Title Page example in student book



*U.S. Department of
Homeland Security*

United States
Secret Service

Title Page

Item	Description
Title (To:)	Indicates report's recipient and date. This information is usually directly related to charging document or request for service.
From	Identifies report's author, including name, organization, and contact information.
Subject	Indicates type of work performed, as well as any suspect and/or local case reference information.



*U.S. Department of
Homeland Security*

United States
Secret Service

Title Page

Item	Description
Support Requested or Purpose for Analysis	Concisely states what charges or allegations were addressed by the analysis, charging jurisdiction or entity, with regard to a specific investigation.
Status	Indicates the current case status, usually Open or Closed. This may change nature from a report to a status update.



*U.S. Department of
Homeland Security*

United States
Secret Service

Title Page

Item	Description
Summary of Findings	A short narrative describing type and nature of any evidentiary items located during analysis with respect to specific allegations or charges. Failure to locate items that support allegations should also be indicated here, as well as items that may exonerate.



*U.S. Department of
Homeland Security*

United States
Secret Service

Title Page

Item	Description
Footer	Includes author's name, title/rank, and a "Released" field for approval signature. Footer may include a legal disclaimer. All pages of the report should be numbered in the Page X of X format.



*U.S. Department of
Homeland Security*

United States
Secret Service

Items Analyzed

- Items Analyzed section of report describes in detail physical and/or logical evidence analyzed
- Always include original *and* verified hash values of all evidence items



U.S. Department of
Homeland Security

United States
Secret Service

Physical Items Analyzed

- Manufacturer
- Model, serial, and part number (when possible)
- Item description
- Any specific markings



*U.S. Department of
Homeland Security*

United States
Secret Service

Logical Items Analyzed

- Items Analyzed section of report details images sent for analysis as well as any “original” evidence items
- List image files in addition to physical containers
- Identify by original file name and include hash or other validation mechanism
- See Items Analyzed example in student book



*U.S. Department of
Homeland Security*

United States
Secret Service

Relevant Software (Analysis)

- List all software applications used during forensic examination to process or analyze suspect media
- Ensure to include primary analysis tool
- Identify software version and brief description of software's functionality or use



*U.S. Department of
Homeland Security*

United States
Secret Service

Relevant Software (Suspect)

- Identifying software on suspect's machine necessary component of case
- Include any software that may have created and/or interacted with data of evidentiary value
- Include any software identified as having been deleted
- Pay particular attention to software commonly used to hide data or securely erase data



*U.S. Department of
Homeland Security*

United States
Secret Service

Relevant Software (Suspect)

- Software name and version
- Full path to where application was located on suspect media
- Brief description of program functionality and how it relates to Request for Analysis and/or investigation
- Be prepared to further explain items in this listing during prosecution
- See Relevant Software example in student book



*U.S. Department of
Homeland Security*

United States
Secret Service

Glossary

- Defines technical terms, document formats, and procedure details referenced in report that may not be readily understood by average non-technical reader
- Define only terms integral to understanding of examination findings as presented in report
- See Glossary example in student book



*U.S. Department of
Homeland Security*

United States
Secret Service

Details of Findings

- Provides detailed information about items of evidentiary value found on suspect media
- Information should be thorough, yet concise, and only contain details relevant to request for analysis and/or investigation
- Should *not* contain detailed information about processes executed that did not produce relevant information, unless negative result is relevant
- Information about non-productive processes should be in notes



U.S. Department of
Homeland Security

United States
Secret Service

Organization of Report

- Several different ways to organize report
- May use different organizational strategies for different investigations
- Might, for example, organize report on case that contains many pieces of media by listing all items found on each piece of media as one section
- In other cases, may be more effective to organize data by date and time in chronological order, e.g., cases involving email, chat and downloads



*U.S. Department of
Homeland Security*

United States
Secret Service

Organization of Report

- Another method, organize evidence by its relationship to a particular criminal charge and subject
- Approach works well for criminal prosecution
- Allows prosecutor to quickly see evidence relevant to a particular charge and subject



*U.S. Department of
Homeland Security*

United States
Secret Service

Organization of Report

- Evidence can be ordered or segregated by device
- Good organizational choice for case that has many pieces of media such as a large quantity of CD's or DVD's
- Strategy is not normally best choice when all evidence is located on one device



*U.S. Department of
Homeland Security*

United States
Secret Service

Organization of Report

- If evidence has multiple partitions, could further subdivide results by individual partition
- Detail partition's file format and size
- To further clarify evidence, could divide findings by each user account or profile
- Detail important files, structure, data, and discrepancies
- Explain techniques, methodology, and relevance of information in brief narrative statements whenever possible



*U.S. Department of
Homeland Security*

United States
Secret Service

Organization of Report

- If analysis did not result in discovery of items of evidentiary value, a simple statement should be included stating negative results
- Ensures reader does not misinterpret an omission as failure to conduct full and competent analysis of evidence



*U.S. Department of
Homeland Security*

United States
Secret Service

Organization of Report

- Include techniques used to locate or extract evidence
- Can refer to report if asked in court how a specific piece of evidence was located
- Example, if file found by manual inspection of drive, state this, not every search has to be done with an automated tool
- Take time to develop organized structure before writing
- See Details of Findings example in student book



*U.S. Department of
Homeland Security*

United States
Secret Service

Items Provided

- Details *all* physical items included with report when submitted
- Should include all items specified in Items Analyzed section
- Include items that were generated as a result of analysis, such as a zip disk, floppy disk, or any CD-Rs of findings, as well as any extracted, hard copy documents
- See Items Provided example in student book



*U.S. Department of
Homeland Security*

United States
Secret Service

Use of Hyperlinks

- Hyperlinking is a way to direct readers to items referred to in report on electronic media
- Often not practical to display certain items in actual report
- Example, report may reference offensive, graphic image of child pornography
- Some readers may not have need to view image
- Others may be required to do so in order to confirm existence
- Hyperlink allows those with need to inspect file, while sparing others from having to view it



*U.S. Department of
Homeland Security*

United States
Secret Service

Use of Hyperlinks

- May be so many items of interest, it would be too cumbersome to include all actual images in written report
- In this situation, hyperlink could lead to entire directory that contains multiple files
- If report is included on CD or other large media, use hyperlinks where possible to illustrate items of evidentiary value
- If not familiar with how to hyperlink, see procedure in student book



*U.S. Department of
Homeland Security*

United States
Secret Service

Procedure: Create a Hyperlink in Microsoft Word

- Step/Action in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 2 – Interviewing Techniques

- Cyber Crime Interviews
- Interview Process



*U.S. Department of
Homeland Security*

United States
Secret Service

Cyber Crime Interviews

- Develop leads, confirm events, and obtain a complete picture of crime
- Can help direct investigation
- Assist in understanding nature of the crime, locating more evidence, identifying suspects
- May assist in revealing true scope of investigation
- Can provide information needed to ensure conviction



*U.S. Department of
Homeland Security*

United States
Secret Service

Accusatory versus Non-Accusatory

- Difference between an interview and interrogation
- Purpose of interview:
 - Gather information that will confirm events
 - Develop suspects and leads
 - Identify facts that lead to root causes of incident
 - Not focused on getting an individual to confess



*U.S. Department of
Homeland Security*

United States
Secret Service

Interviews

- Often first and best opportunity to determine what has happened and clarify confusion or misconceptions
- To develop information
- To obtain information
- Develop rapport with subjects
- Conducted in non-confrontational manner



*U.S. Department of
Homeland Security*

United States
Secret Service

Interrogations

- Focus on presenting facts of case and eliciting statements that confirm suspect's involvement



*U.S. Department of
Homeland Security*

United States
Secret Service

Accusatory versus Non-Accusatory

- Accusatory approach may inhibit effective communication
- Take into account perceptions of interviewees
- Many people you will encounter during initial interviews have little to no exposure to law enforcement outside of television
- People may view interaction with government agents through lens of personal attitudes, experiences, and beliefs about law enforcement
- Law enforcement often cast in negative light and government agents seen as dimwitted and overbearing



*U.S. Department of
Homeland Security*

United States
Secret Service

Interview Process

- Planning/Research
- Opening/Rapport
- General Questioning
- Detailed Questioning
- Interview Termination



*U.S. Department of
Homeland Security*

United States
Secret Service

Planning and Research

- Conduct preliminary research on interviewee and organization
- Helps to draft appropriate questions and an interviewing approach that will be successful
- knowledge and comprehension of technical subject's area of expertise presents professional and approachable image
- Knowledge gained through planning and research enables interviewer to ask more intelligent questions



*U.S. Department of
Homeland Security*

United States
Secret Service

Opening/Rapport

- The initial contact is critical to obtaining cooperation
- Showing respect for individual and organization and explaining importance of questions, vital steps in obtaining cooperation
- Explain to interview subjects that you need assistance in determining facts of case and understanding issues involved



*U.S. Department of
Homeland Security*

United States
Secret Service

General Questioning

- Start with open-ended questions that allow subject to explain his/her knowledge of events
- Questions should develop a general framework of incident derived from subject's personal knowledge of factual events
- Important to obtain general outline of events that transpired to document information relevant to case



*U.S. Department of
Homeland Security*

United States
Secret Service

General Questions Address

- Key incidents that brought situation to light
- Hardware involved (routers, firewalls, IDS)
- Specific individuals involved in incident and actions they took with any evidence
- Physical locations of effected machines and people
- Technology that will need clarification during Detailed Questioning phase



*U.S. Department of
Homeland Security*

United States
Secret Service

Detailed Questions Address

- Software and hardware model numbers and versions
- Network monitoring and logging setup
- Collection of current logs
- Network diagrams
- User policies
- List of people who had logical and physical access



*U.S. Department of
Homeland Security*

United States
Secret Service

Detailed Questions Address

- Ownership and authorized access of systems
- User account information
- Statements of how systems are used
- Individual access to relevant systems and/or data
- Specific commands or tools used during discovery of incident
- Security video or proximity card logs



*U.S. Department of
Homeland Security*

United States
Secret Service

Interview Termination

- Thank subject for time and cooperation
- Ask subject for contact information in case need arises for clarification of material discussed during interview



*U.S. Department of
Homeland Security*

United States
Secret Service

Interview Psychology

- Take into account subject's perspective and culture
- Establish tone for interview, important in obtaining all necessary information available from subject
- Approach may differ depending on whether investigator initiates contact for information or investigator is called by organization
- Issue influences how investigator structures approach to interviews



*U.S. Department of
Homeland Security*

United States
Secret Service

Interview Psychology

- When organization calls in investigator, most of organization's key players already involved
- Management typically supports initial stages of investigation
- Obtain written documentation from everyone involved and begin working on controlling investigation
- Important to minimize mishandling or destruction of evidence and spread of information



*U.S. Department of
Homeland Security*

United States
Secret Service

Investigator Initiated Contact

- Identify point of contact within organization
- Look up registration information for company via Internet search engine and identify legal counsel and network administrator
- Variety of state, federal, and private registries contain information and provide it to law enforcement agencies
- Several Internet service provider lists include contact information for major communications providers such as AOL, Microsoft, Google, Yahoo, and others



*U.S. Department of
Homeland Security*

United States
Secret Service

Investigator Initiated Considerations

- Is system administrator or someone with root access responsible for activity?
- Do they know suspect and are they relaying information about the investigation to their associate?
- Are there any regulatory or legal barriers to organization providing information (ECPA, PPA, FERPA, HIPPA, Organizational Policy, etc.)
- How critical is evidence held by company to the case?
- Is a life or national security at stake?



*U.S. Department of
Homeland Security*

United States
Secret Service

Investigator Initiated Considerations

- Access to legal instruments such as subpoenas, search warrants, FISA, or other items in timely manner?
- Technical knowledge to handle systems or logs that will be obtained from scene or require assistance?
- Evidence contained or spread out over national or global network infrastructure?
- Manpower, technical knowledge, and resources to obtain what's needed from target organization?



*U.S. Department of
Homeland Security*

United States
Secret Service

Investigator Initiated Considerations

- Best to identify senior management, legal counsel, and technical heads prior to making contact
- Start at top of organization's hierarchy and work down towards individuals responsible for managing or using various computer and network services
- Address legal issues, business impact, and concern for organization's needs in order to gain more cooperation



*U.S. Department of
Homeland Security*

United States
Secret Service

Investigator Initiated Considerations

- If an investigation could be compromised by reaching out avoid “tipping off” organization or individuals
- Do research and case preparation to obtain most effective legal authority that will allow gathering evidence and interviewing in most effective and efficient manner



*U.S. Department of
Homeland Security*

United States
Secret Service

Organization Initiated Contact

- Investigator will more likely have cooperation
- Victim may have performed internal investigation that may or may not have been done properly
- Still need to follow up to ensure accuracy of any information provided
- Document any actions taken by people at company
- Important to work with legal counsel and network administrators



*U.S. Department of
Homeland Security*

United States
Secret Service

Organization Initiated Contact

- Many organizations ignorant of investigation's process and do not use proper evidence handling procedures
- Common practices used by organizations to minimize or repair damage often hamper investigation



*U.S. Department of
Homeland Security*

United States
Secret Service

Organization Initiated Concerns

- When compromised it is common practice to just restore machine from base image
- Often untrained system administrators or management work on live systems and alter artifacts and time lines
- More concern for system/network integrity compared to retaining evidence or identifying cause of incident



*U.S. Department of
Homeland Security*

United States
Secret Service

Organization Initiated Concerns

- Chain of custody issues are often not followed
- Lack of network maps and diagrams
- Incomplete knowledge of system functions and passwords
- Poor documentation of system builds, organizational policies, or security controls



*U.S. Department of
Homeland Security*

United States
Secret Service

Witness and Victims

- Often provide investigator initial foundation of case and information needed to build framework for investigation
- System administrator or user of an online database may be first to notice strange behavior or altered data
- A relative or friend may discover suspected child pornography images on a computer
- In either situation, investigator needs to elicit information from people to obtain facts that will lead them to suspect



*U.S. Department of
Homeland Security*

United States
Secret Service

Witness and Victims

- Keep in mind, anyone could be a suspect
- During initial response and interviews, obtain clear and concise written documentation from people involved
- Documentation should consist of any actions taken by witnesses and events observed during incident
- Documentation is important part of freezing crime scene and creating permanent record of events that occurred during and subsequent to discovery of crime



*U.S. Department of
Homeland Security*

United States
Secret Service

Witness and Victims

- People being interviewed may have had little contact with law enforcement and may not recognize evidence needed to further investigation
- Develop a rapport with interview subjects and guide interview in direction that will obtain most relevant and complete information available



*U.S. Department of
Homeland Security*

United States
Secret Service

Issues to Address

- System administrators or people with administrative powers may be potential suspects
- Move quickly and efficiently to build case
- If immediate action is not an option, ensure that suspect's access to evidence or sensitive material is removed
- Covert tactics may be necessary if you have proper administrative approval, legal documents, and technical capabilities in place



*U.S. Department of
Homeland Security*

United States
Secret Service

Issues to Address

- Obtaining witness statements about suspect's access to machine or data is important
- Supplement network logs and/or forensic analysis with as much traditional detective work as possible
- Determine if people share machines, use passwords, or share passwords
- Recent attempts at social engineering, phone calls or any person asking for user accounts, passwords, or other sensitive technical information



*U.S. Department of
Homeland Security*

United States
Secret Service

Suspects

- Traditionally, investigators interview victim and eventually a suspect
- In cyber crime cases, can be unclear who is victim or who is a suspect
- Investigator must use analytical skills to determine who should be interviewed during an investigation and best approach to take



*U.S. Department of
Homeland Security*

United States
Secret Service



*U.S. Department of
Homeland Security*

United States
Secret Service

Module 11 – Legal Issues



*U.S. Department of
Homeland Security*

United States
Secret Service

You Will Learn . . .

- Search Warrants
- Internet Service Providers



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 1 – Search Warrants

- Affidavit
- Warrant



*U.S. Department of
Homeland Security*

United States
Secret Service

Search Warrants

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”



U.S. Department of
Homeland Security

United States
Secret Service

Search Warrants

- Authorization for search and seizure from approving authority prior to execution of activities
- Provide most reliable means of obtaining evidence
- Properly crafted and executed, difficult to overcome
- Preferred by Supreme Court when probable cause to believe a crime has been committed and seeking search authority



*U.S. Department of
Homeland Security*

United States
Secret Service

Obtaining a Search Warrant

- Be familiar with Federal Rules of Criminal Procedure Rule 41, “Search and Seizure”
- Investigator who requests search warrant must establish by sworn affidavit some key pieces of information
- Failure to establish any of these facts can result in search warrant being denied or overturned



*U.S. Department of
Homeland Security*

United States
Secret Service

Facts for Issuance of Search Warrant

- Description of place to be searched
- Concise description of item(s) being sought
- Probable Cause or facts that support belief that items being sought are located in place described



*U.S. Department of
Homeland Security*

United States
Secret Service

Example Search Warrant

- A copy of a modern federal search warrant is found as an editable PDF format at:
- <http://www.uscourts.gov/forms/AO093.pdf>



*U.S. Department of
Homeland Security*

United States
Secret Service

Affidavit

- Warrant typically accompanied by an attached affidavit
- Affidavit will normally contain the following components:
 - The affiant's statement of probable cause
 - Attachment A – Place To Be Searched
 - Attachment B – Items To Be Seized



*U.S. Department of
Homeland Security*

United States
Secret Service

Format

- No formally required format for typical affidavit attachments, though various agencies and jurisdictions may follow formats developed over time
- Warrant will generally give brief statements of affidavit components and refer to affidavit for greater detail
- See example in student book



*U.S. Department of
Homeland Security*

United States
Secret Service

(CCIPS) Guide for Warrants

- United States Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), publishes useful guide called Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations
- Publication is available in hardcopy, and online at:
<http://www.cybercrime.gov/s&smanual2002.htm>



*U.S. Department of
Homeland Security*

United States
Secret Service

(CCIPS) Guide for Warrants

- Appendix F of CCIPS publication, *Sample Language for Search Warrants and Accompanying Affidavits to Search and Seize Computers*, is de facto standard for warrant/affidavit language in federal cyber investigations



U.S. Department of
Homeland Security

United States
Secret Service

Description of Place to be Searched

- 4th Amendment requires investigator to concisely identify and define search location in physical terms
- Often difficult to do in cyber crime investigation as physical and virtual worlds may not share same physical space
- Goal is to define boundaries of search location in manner that area within those boundaries may be searched, but search is not overly broad
- See examples in student book



*U.S. Department of
Homeland Security*

United States
Secret Service

Description of Item(s) to be Seized

- Investigators crafting a search warrant affidavit should carefully consider description of items sought in seizure
- In most cyber crime cases, item sought is basically information
- If information can be described, different forms it may take and different storage media upon which it may reside, may more easily be articulated
- Must establish probable cause in sworn affidavit for each item to be seized
- See example in student book



*U.S. Department of
Homeland Security*

United States
Secret Service

Execution of a Search Warrant

- Once warrant is signed by judge, it may be served, search initiated, and evidence collected
- Most court jurisdictions require investigator to submit a Search Warrant Return document to the court describing items actually seized



*U.S. Department of
Homeland Security*

United States
Secret Service

Surreptitious Execution of Warrant

- In some cases, such as those involving organized crime figures, or violent individuals, may want to execute warrant without knowledge of individual and without public disclosure of warrant or affidavit until trial
- In these cases, a surreptitious entry warrant may be requested and issued



*U.S. Department of
Homeland Security*

United States
Secret Service

Surreptitious Execution of Warrant

- Surreptitious entry warrant authorizes investigator to enter premises and conduct search without individual's knowledge
- Affidavits, search warrants, and Search Warrant Return are kept under seal and not made public
- Similar physical search authority can be issued under FISA provision in accordance with the USA PATRIOT ACT



*U.S. Department of
Homeland Security*

United States
Secret Service

Search Warrant Exceptions

- U.S. Supreme Court has interpreted specific exceptions for 4th Amendment requirement to obtain a search warrant
- Know and understand circumstances under which search of individual or premises authorized without warrant



*U.S. Department of
Homeland Security*

United States
Secret Service

Warrant Exceptions

- Consent
- Stop and Frisk
- Search Incident to Arrest
- Immediate threat to life or serious bodily injury
- Immediate threat of the destruction of evidence



*U.S. Department of
Homeland Security*

United States
Secret Service

Warrant Exceptions

- Fresh pursuit
- Plain view
- Vehicle searches
- Custodial searches
- Border searches



*U.S. Department of
Homeland Security*

United States
Secret Service

Consent Searches

- Person may waive rights under 4th Amendment and consent to search of his person or items under his control
- Most common exception to warrant clause
- Evidence obtained during consent search is admissible in court as long as investigator obtained proper consent
- Investigators should understand how consent is granted and limitations



*U.S. Department of
Homeland Security*

United States
Secret Service

Owner Consent

- Property owner has legal authority to authorize search of premises as long as certain requirements are met:
 - Consent must be voluntary and not coerced
 - Consent must be informed
 - Consent can be withdrawn at any time
 - Consent can be limited



*U.S. Department of
Homeland Security*

United States
Secret Service

Owner Consent

- When consent search is granted, should be obtained in writing, signed by consenting party, dated with known good local time and location
- Most agencies have consent search form for this purpose



*U.S. Department of
Homeland Security*

United States
Secret Service

Voluntary Consent

- To be valid, owner must consent freely and knowingly
- Investigator may ask for consent to search
- If permission granted by owner, investigator may search property or premises legally
- Cannot coerce owner by threats, intimidation, or power of authority into consenting to search



*U.S. Department of
Homeland Security*

United States
Secret Service

Informed Consent

- Not everyone capable of giving consent to search
- Some are legally and mentally incompetent, unfit to make such a decision
- Those with clinically diagnosed mental conditions and severe health problems that affect judgment, unable to intelligently consent
- Minors generally not trusted to give consent
- Be familiar with court decisions in your area concerning informed consent to search



*U.S. Department of
Homeland Security*

United States
Secret Service

Withdrawing Consent

- Person who waives 4th Amendment rights can reassert rights any time by telling investigator to stop search
- Investigator must stop search unless in possession of some other legal authority to continue search
- Evidence located before consent is withdrawn is admissible and can be retained investigator for further analysis



*U.S. Department of
Homeland Security*

United States
Secret Service

Withdrawing Consent

- Prioritize places to search and items to seize when operating under consent search in case consent is withdrawn
- Maximize the effectiveness of search in the event consent is withdrawn
- Forensic copies of computer evidence should be made as soon as possible in consent cases



*U.S. Department of
Homeland Security*

United States
Secret Service

Third Party Consent

- Possible to obtain consent from third party for areas which are communal to target and third party
- Third party must have ownership or right to access search area
- Search area may apply to computers when multiple users share single account
- If no shared account, third party can only consent to search of his or her account or shared storage space under his or her control



*U.S. Department of
Homeland Security*

United States
Secret Service

Third Party Consent

- Spouses can generally consent to search of other spouse's property
- True as long as target has not asserted exclusive rights to search area
- Absent evidence to contrary, investigators can rely upon consenting spouse's assertion to authority in good faith, even if consenting spouse later deemed not to have authority to grant consent



*U.S. Department of
Homeland Security*

United States
Secret Service

Third Party Consent

- Parents can generally consent on behalf of juveniles living in premises under parent's control
- Landlords generally do not have authority to authorize search of rented property unless such consent is authorized under a rental agreement with tenant



*U.S. Department of
Homeland Security*

United States
Secret Service

Third Party Consent

- Military commanders or magistrates can authorize search of military facilities under their command, including search of persons on those facilities
- System administrators may consent to search of an entire computer or network over which they have administrative privileges



*U.S. Department of
Homeland Security*

United States
Secret Service

Immediate Threat to Life or Serious Bodily Injury

- Investigator may enter and search premise without warrant when there is immediate threat to life or serious bodily injury
- Exception allows investigator to come to immediate rescue of individual in peril
- While legally inside premises, investigator can legally seize evidence that may be discovered during rescue attempt



*U.S. Department of
Homeland Security*

United States
Secret Service

Immediate Threat of the Destruction of Evidence

- An investigator may enter a premise without a warrant to stop immediate destruction of evidence in a criminal investigation
- Threat must be immediate



*U.S. Department of
Homeland Security*

United States
Secret Service

Fresh Pursuit

- An investigator in pursuit of an individual may follow individual into or through a premise
- If evidence of a crime is observed during pursuit, investigator may legally seize evidence



*U.S. Department of
Homeland Security*

United States
Secret Service

Plain View

- Investigator has the right be in a physical place
- Evidence of a crime visible may be seized without a warrant
- Is admissible in court of law



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 2 – ISP's

- Preservation Letters
- Subpoenas
- Search Warrants
- Available Data
- Retention Schedules



*U.S. Department of
Homeland Security*

United States
Secret Service

Internet Service Providers' Records

- Many crimes involve use of commercial and private networks and communications facilities
- Records usually maintained by Internet Service Providers (ISPs)
- Records of accounts, billing, transactions, and content of the communications and data
- Might need to gather this pertinent information from ISPs
- Should understand proper way to request records so they are admissible as evidence in a criminal proceeding



*U.S. Department of
Homeland Security*

United States
Secret Service

Access to Records

- Access to stored wire and electronic communications and transactional records, governed by Chapter 121 of U.S. Code (currently comprised of 18 USC § 2701-2711)
- Enacted in 1986 by the Electronic Communications Privacy Act (ECPA)
- ECPA defines how government can obtain stored account information from third parties



*U.S. Department of
Homeland Security*

United States
Secret Service

ECPA Three Information Categories

- Basic Subscriber Information - 18 U.S.C. § 2703(c)(2)
- Records or Other Information Pertaining to a Customer or Subscriber - 18 U.S.C. § 2703(c)(1)
- Contents



*U.S. Department of
Homeland Security*

United States
Secret Service

Basic Subscriber Information

- Name and Address
- Telephone connection records, session times and durations
- Length of service and types of service utilized
- Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
- Means and source of payment for such service (including any credit card or bank account number)



*U.S. Department of
Homeland Security*

United States
Secret Service

Records or Other Information

- A catch-all for anything else that is not content



*U.S. Department of
Homeland Security*

United States
Secret Service

Contents

- When used with respect to any wire, oral, or electronic communication, includes any information concerning substance, purport, or meaning of that communication



*U.S. Department of
Homeland Security*

United States
Secret Service

Mechanisms to Compel Disclosure

- See table in student book, reproduced from U.S. DOJ publication Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations



*U.S. Department of
Homeland Security*

United States
Secret Service

Express Consent

- Derived from an individual's actions as result of documents and notices provided to individual before an incident occurs
- Type of consent usually seen in logon banners or signs advising that use of system or entry “implies” consent to be monitored or searched
- Act of entry onto system or property constitutes informed, voluntary consent



*U.S. Department of
Homeland Security*

United States
Secret Service

Authority and Ownership

- During initial investigation of a cyber crime, firmly establish owner or Designated Authorization Authority of any computer or network involved
- Ownership or authority should be documented in report and verified by supporting documentation in form of policies, orders, copies of ownership records or written statements



*U.S. Department of
Homeland Security*

United States
Secret Service

Establishing and Documenting Express Consent

- When a user logs onto a computer or network, there may be an initial warning banner that explains authority to access computer or network as well as any implications such access may have for the user
- Banner should require some type of action by user to acknowledge its presence and acceptance of terms
- Banners that flash and disappear without user interaction may not suffice to establish express consent



*U.S. Department of
Homeland Security*

United States
Secret Service

Record Retention

- Storage and destruction of electronic logs and records, much more dynamic than traditional methods of recordkeeping
- Takes time to obtain court orders (up to and including warrants)
- No federal laws that require companies to preserve electronic records for any amount of time
- Some companies maintain records and logs for months, some not at all



*U.S. Department of
Homeland Security*

United States
Secret Service

Preservation Request

- Part of ECPA is designed to ensure available data is not lost during time it takes to obtain preservation order
- Request can be issued quickly and directly for preservation of information for 90 days
- Designed to ensure the specified information will still be there when appropriate legal process is served



*U.S. Department of
Homeland Security*

United States
Secret Service

18 USC § 2703(f)(1)

“A provider of wire or electronic communication service or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.”

- No required format for § 2703(f) requests
- Most agencies have developed their own preferred format, usually in form of a letter
- Technically, request can be verbal



U.S. Department of
Homeland Security

United States
Secret Service

Subpoena

- Court order requiring a person or business entity to produce records or testimony
- Failure to comply with subpoena may result in penalties or criminal charges
- Used to obtain stored transactional records (basic subscriber information) and in some circumstances, stored wire and electronic communications (content)



*U.S. Department of
Homeland Security*

United States
Secret Service

Obtaining a Subpoena

- In a cyber crime investigation, investigator can request issuance of subpoena for records under control of an individual or business
- Prosecutor has authority to issue the subpoena and have the person or business served with the document
- Once served, individual or business has right to argue before a competent court of jurisdiction why records should not be produced



*U.S. Department of
Homeland Security*

United States
Secret Service

“D” Order

- Standard of proof to obtain court order under 18 U.S.C. § 2703(d) is higher than for a subpoena, but lower than for a warrant
- Information that can be obtained with a “D” order falls between that which can be obtained by the subpoena and the warrant
- Commonly used to obtain stored transactional records and stored wire and electronic communications (content)



*U.S. Department of
Homeland Security*

United States
Secret Service

Obtaining a “D” Order

- 18 USC § 2703(d) states that a court order for the disclosure of customer records may be issued after the following has been submitted:

“..specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.”



U.S. Department of
Homeland Security

United States
Secret Service

Obtaining a “D” Order

- Orders issued under statute generally used to obtain Basic Subscriber Information and Records or Other Information Pertaining to a Customer or Subscriber, but not for content
- Investigators should coordinate with prosecutors to obtain a D order
- Investigator will submit affidavit to apply for order
- Affidavit should meet requirements set forth in section (d)



*U.S. Department of
Homeland Security*

United States
Secret Service



*U.S. Department of
Homeland Security*

United States
Secret Service

Module 12 – Fundamentals of Log Analysis



*U.S. Department of
Homeland Security*

United States
Secret Service

You Will Learn . . .

- Understanding Network Traffic
- The Scientific Method and Intrusion Analysis
- Observing Intrusion-related Activity and Generating a Hypothesis
- Predicting the Nature and Location of Intrusion Artifacts
- Using Log Analysis to Evaluate an Intrusion Hypothesis



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 1 – Understanding Network Traffic

- Overview of Network Traffic
- Investigation Techniques



*U.S. Department of
Homeland Security*

United States
Secret Service

The Internet

- TCP/IP is the language of the Internet
- Number of services which use TCP/IP to communicate
- Example of one service, HyperText Transfer Protocol (HTTP)



*U.S. Department of
Homeland Security*

United States
Secret Service

Network Communication

- To generate network traffic one system must serve or host information and another system request the service data
- In the case of HTTP there is a web server and a web client
- Network traffic is generated when client or browser requests a web page from the server



*U.S. Department of
Homeland Security*

United States
Secret Service

Network Communication

- *SYN*: Client sends Synchronize packet to server, beginning three-way handshake which starts conversation
- *SYN-ACK*: Server sends Synchronization Acknowledgement, acknowledging start of conversation
- *ACK*: Client sends acknowledgement to server completing three-way handshake, conversation started



*U.S. Department of
Homeland Security*

United States
Secret Service

Network Communication

- *GET*: Client requests page from server
 - If general request to web site like www.somewhere.com GET request is for web root document indicated with a backslash / after get command
 - Otherwise name of page will be part of get request, such as [faq.html](#)



*U.S. Department of
Homeland Security*

United States
Secret Service

Network Communication

- *200 OK*: Server will send response that includes status code for page requested
 - Usually code 200 OK is sent
 - Indicates page found and will immediately follow
 - Page transferred to browser program and displayed on client system
- *404 Page not found*: If specific page requested is not recognized by server, 404 page not found displayed in browser



*U.S. Department of
Homeland Security*

United States
Secret Service

Ports in a Data Storm

- There are 65535 port numbers available on most computer systems
- The Internet Assigned Numbers Authority (IANA) has role of assigning types of traffic to port numbers
- Assignments done so programmers can agree on ports used for specific types of traffic
- HTTP traffic assigned port 80



*U.S. Department of
Homeland Security*

United States
Secret Service

Types of Ports

- Three types of port numbers, Well Known, Registered and Dynamic Ports
- Well Known Ports are numbers ranging from 0 to 1023
- Registered Ports are numbers ranging from 1024 to 49151
- Dynamic Ports are numbers ranging from 49152 to 65535
- Documentation on current assignment of numbers can be viewed by going to www.iana.org/assignment/port-numbers



*U.S. Department of
Homeland Security*

United States
Secret Service

Common Well Known Ports

- (20) File Transfer Protocol (FTP)
- (21) File Transfer Control (FTP)
- (22) Secure Shell Remote Login
- (23) Telnet



*U.S. Department of
Homeland Security*

United States
Secret Service

Common Well Known Ports

- (25) Simple Mail Transfer Protocol (SMTP E-mail)
- (53) Domain Name Service (DNS)
- (80) HTTP (Web)
- (443) Secure Socket Layer (HTTPS)



*U.S. Department of
Homeland Security*

United States
Secret Service

Common Assigned Ports

- (1025) Network Blackjack
- (1080) SOCKS
- (1169) Tripwire
- (1214) KAZAA
- (1433) Microsoft SQL Server
- (1689) Firefox



*U.S. Department of
Homeland Security*

United States
Secret Service

Investigation Techniques

- Look for traffic types that are on wrong assigned ports
- For example AOL Instant Messenger traffic on port 80
 - AOL IM is assigned port 531



*U.S. Department of
Homeland Security*

United States
Secret Service

Types of Traffic to Watch For

- HTTP (port 80)
 - Most firewalls and routers will pass traffic on port 80
 - Popular port for malicious code transfer, or for communication of other protocols that have been blocked
 - May see programs that opened backdoors on systems transferring information on port 80
 - Advanced attackers might embed malicious code in HTTP packets hoping firewalls and intrusion detection systems will pass the information



*U.S. Department of
Homeland Security*

United States
Secret Service

Types of Traffic to Watch For

- E-mail (port 25)
 - Not a common port for traffic other than e-mail
 - Port is worth watching simply because so many attacks originate in e-mail messages



*U.S. Department of
Homeland Security*

United States
Secret Service

Types of Traffic to Watch For

- USENET/NNTP (port 119)
 - Important protocol for law enforcement to watch
 - Newsgroups are used for distribution of pornography in all forms
 - Protocol still used as way to transfer bootleg software, movies, music and other copyrighted material



*U.S. Department of
Homeland Security*

United States
Secret Service

Types of Traffic to Watch For

- Internet Relay Chat (ports 6666-6669)
 - IRC is another protocol used heavily for Peer-to-Peer transfer of copyrighted and illicit materials
 - Malware and Botnet traffic seen on these ports as well



*U.S. Department of
Homeland Security*

United States
Secret Service

Types of Traffic to Watch For

- File Transfer Protocol (port 21)
 - FTP used for transferring files
 - If case involves transfers of illicit information of any kind monitor FTP traffic
 - There are a number of malware attacks against FTP ports as well



*U.S. Department of
Homeland Security*

United States
Secret Service

Types of Traffic to Watch For

- Peer-to-Peer (Any ports)
 - P2P protocols are some of the hardest to monitor and investigate
 - Two systems that are transferring information can use any port they agree on
 - Transfer of a file may actually take place between multiple systems at once
 - Reassembly of transferred files can be extremely difficult



*U.S. Department of
Homeland Security*

United States
Secret Service

Baselines

- Popular way to make network traffic analysis easier is baseline method
- Method involves taking packet capture snapshots of normal network traffic and comparing suspicious traffic captures to baseline
- Helps to quickly determine where investigation should focus



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 2 – The Scientific Method and Intrusion Analysis

- Overview of the Scientific Method
- Digital Forensic Analysis and the Scientific Method



*U.S. Department of
Homeland Security*

United States
Secret Service

Scientific Method

- A process for investigating a set of observations
- Formulating a hypothesis about observed events
- Using deductive/inductive logic to formulate processes for evaluating hypothesis
- Carrying out processes and using results to support, contradict, or modify hypothesis



*U.S. Department of
Homeland Security*

United States
Secret Service

Scientific Method Steps

- *Observation:* Observing one or more events or sets of events, establish facts surrounding events to identify cause and consequences
- *Hypothesis:* Explains observed events, including root cause, interrelationship, and consequences
- *Prediction:* Possible nature and location of artifacts in evidence that will either support or contradict hypothesis
- *Evaluation:* Procedures that test for presence of artifacts that support, falsify, or modify the hypothesis



U.S. Department of
Homeland Security

United States
Secret Service

Scientific Method Steps

- *Conclusion:* Based upon results of tests performed during Evaluation step, stating one of following:
 - Hypothesis is supported by facts
 - Hypothesis is contradicted by facts
 - Facts indicate that new or modified hypothesis should be constructed due to observations or lack of relevant results



U.S. Department of
Homeland Security

United States
Secret Service

Additional Characteristics

- *Repeatable*: Evaluations and tests conducted should be repeatable to ensure results can be verified by others who want to test for mistakes, confounding variables, spurious relationships, etc.
- *Cyclic*: May need to perform many iterations of method, tests, and testing of hypothesis, or generate additional hypothesis to gain a clear understanding of originally observed events



U.S. Department of
Homeland Security

United States
Secret Service

Additional Characteristics

- *Empirical*: Evidence used in hypothesis must be based on or derived from observation rather than pure reasoning, faith, common sense, etc
- *Falsifiable*: Hypothesis established and tested using Scientific Method should be falsifiable, there should be way to test for contradicting evidence as well as supporting evidence
- *Objectivity*: Observations and results of evaluations must be interpreted as objectively as possible



U.S. Department of
Homeland Security

United States
Secret Service

Variances

- Not all fields of inquiry use same steps for Scientific Method, names of steps can differ
- When researching method, you might encounter different formats within different reference sources
- Implementation of Scientific Method is valid so long as it follows principles outlined previously



*U.S. Department of
Homeland Security*

United States
Secret Service

Digital Forensic Analysis and the Scientific Method

- Scientific Method provides useful guide when attempting to locate items of interest within digital media, or copies of digital media
- Useful for incident responder when attempting to identify devices that may contain information related to series of events



*U.S. Department of
Homeland Security*

United States
Secret Service

Example of Application

- Incident responder responds to several IDS alerts indicating attack against Web server
- Alerts are initial *observations*
- Responder might form a *hypothesis* that Web server attacked and compromised by method indicated in alerts
- To test hypothesis, analyst deduces (*predicts*) most probable location of artifacts to support or contradict hypothesis that system was successfully attacked



U.S. Department of
Homeland Security

United States
Secret Service

Example of Application

- Supporting artifacts might include unauthorized Registry entries, presence of malicious code, additional IDS alerts, unauthorized user accounts, etc
- Contradicting artifacts could be other log entries that show observed events part of normal activity for an application
- Analyst gathers data from devices containing artifacts, and *evaluates* data for their presence



U.S. Department of
Homeland Security

United States
Secret Service

Example of Application

- Examiner finds artifacts that support hypothesis that system was successfully attacked
- *Concludes* that hypothesis was correct, proceeds to write report
- Alternatively, hypothesis may have been falsified due to discovery of artifacts indicating legitimate technical reason for IDS alerts such as standard false positive
- Investigator may not find sufficient evidence to make any conclusion in which case he/she may create a new hypothesis



U.S. Department of
Homeland Security

United States
Secret Service

Use of Scientific Method for Computer Intrusion Investigations

- Computer network intrusions can be complex, difficult to track
- Attack can span multiple networks, thousands of systems
- Danger for investigative team is spending too much time acquiring and analyzing data from unrelated systems
- Scientific Method helps avoid pitfall by encouraging use of a logical process to determine approach to investigation



*U.S. Department of
Homeland Security*

United States
Secret Service

Use of Scientific Method for Computer Intrusion Investigations

- Key element is link between observed events and subsequent investigative tasks
- Creating hypotheses based on observations and events, makes it more likely you will perform analysis tasks that produce results, less likely you will follow unproductive tangents



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 3 – Observing Intrusion-related Activity and Forming a Hypothesis

- Common Observations
- Hypothesis Formation
- Incident Classification



*U.S. Department of
Homeland Security*

United States
Secret Service

Observations and Network Intrusions

- Network intrusion investigations should normally begin with one or more observation
- Observations guide formation of hypothesis as to what occurred



*U.S. Department of
Homeland Security*

United States
Secret Service

Common Primary Observations

- Antivirus alerts
- IDS/IPS alerts
- System/applications errors
- Abnormal authentication patterns
- Access control list violations
- Generic unusual activity



*U.S. Department of
Homeland Security*

United States
Secret Service

Supplementary Observations

- Incident responder should make supplementary observations before creating hypothesis
- Not directly observed events, rather sets of data that responder should collect in any security incident



*U.S. Department of
Homeland Security*

United States
Secret Service

Supplementary Observations

- Network diagrams: Logical and physical diagrams of networks
- Device documentation: Lists of device names and configuration data, vital for devices directly involved in events
- Contact information: Names, phone numbers, e-mail addresses, etc. for witnesses and people responsible for affected networks and systems
- Other data: Other details regarding affected devices and networks that may seem pertinent



*U.S. Department of
Homeland Security*

United States
Secret Service

Common Observation Attributes

- Date/time: Record when event occurred, as well as duration
- IP addresses: If event is log entry that includes an IP address, or involves system with IP address, IP addresses should be recorded
- Port numbers: If event is log entry that includes port numbers, or involves application that engages in network communication over specific port, ports should be recorded
- Host names and aliases: Host names and aliases for systems involved in event should be recorded



*U.S. Department of
Homeland Security*

United States
Secret Service

Common Observation Attributes

- Accounts and aliases: Specific user account or alias, should be recorded, as well as names of specific individuals that use account or alias, if information known
- Files: At minimum, name and full path for any files involved, attributes, hash values, file system date/time stamps
- General description: General description as to nature of each event



*U.S. Department of
Homeland Security*

United States
Secret Service

Hypothesis Formation

- What/How - Basic description of main event(s), may include common incident classification
- Where - List known and probable physical locations and network segment locations of incident
- When - List known and probable timeframe of incident
- Who - List identifying information for individual(s)/computer(s) known to be involved or likely involved in incident
- Why - List most likely motive(s)



*U.S. Department of
Homeland Security*

United States
Secret Service

Multiple Hypotheses

- Incident may be too large and complex for single hypothesis
- May need to establish multiple hypotheses to account for different parts of incident
- For instance, intrusion may have signs that attacker entered through public Web server and several compromised workstations
- To effectively pursue each possibility, could create a hypothesis for each potential method of entry



*U.S. Department of
Homeland Security*

United States
Secret Service

Multiple Hypotheses

- Managers or lead investigators, may assign different investigators to investigate each hypothesis
- Could create third hypothesis to account for how attacker(s) are extracting stolen data from network
- No rule for determining how many hypothesis to create or how detailed
- Hypotheses should reflect the size and complexity of incident



*U.S. Department of
Homeland Security*

United States
Secret Service

Incident Classifications

- Implement an incident classification schema to ensure a common vocabulary between agency and organization requesting assistance
- Classification should be broad enough to capture major types of incidents



*U.S. Department of
Homeland Security*

United States
Secret Service

Common Incident Classification

- Denial of Service
- Malicious Code
- Unauthorized Access
- Inappropriate usage
- Suspicious activity
- Multiple Component
- Other



*U.S. Department of
Homeland Security*

United States
Secret Service

Denial of Service

- Prevents or impairs authorized use of networks, systems, or applications
- Network service is unavailable for an unknown reason
- Computer network saturated with excessive amount of traffic
- Application saturated with authentication or service requests
- Application or operating system not functioning for unknown reason



*U.S. Department of
Homeland Security*

United States
Secret Service

Malicious Code

- Program or group of programs that perform undesirable activity
- Antivirus alerts
- IDS alerts that indicate malicious code
- A higher than normal volume of network traffic
- Computer systems crash or malfunction for unknown reason
- Egress communication not initiated by user or authorized application



*U.S. Department of
Homeland Security*

United States
Secret Service

Unauthorized Access

- Person gains logical or physical access without permission to network, system, application, data, or other resource
- User account authentication at abnormal times, or at times user to which account assigned denies having been on system
- Presence of unauthorized user accounts
- Missing data



*U.S. Department of
Homeland Security*

United States
Secret Service

Unauthorized Access

- Logged data access at abnormal times or by user account not normally used for such access
- Presence of unauthorized computer programs
- Presence of large archives (TAR, RAR, Zip, etc.) of data files for which there is no explanation
- Common observations from any other type of intrusion-related activity



*U.S. Department of
Homeland Security*

United States
Secret Service

Inappropriate Usage

- Violations of acceptable computing use policies
- Web browsing sessions to websites containing unauthorized workplace material
- Inappropriate e-mails sent to coworkers or from a work account
- Recorded network traffic that indicates presence of unauthorized application, such as a peer-to-peer file sharing application



*U.S. Department of
Homeland Security*

United States
Secret Service

Suspicious Activity

- Security operations personnel notice unusual activity not specifically related to known threat, unexplainable through experience
- Increase network activity
- Increase CPU activity on a system
- Unexplained network activity



*U.S. Department of
Homeland Security*

United States
Secret Service

Multiple Component

- Multiple component classification, situation that encompasses two or more incidents out of one
- For example, malicious code infection leads to unauthorized access to host, used to gain unauthorized access to additional hosts
- Workstation affected by a virus and scanning the network
- Server relaying IRC traffic



*U.S. Department of
Homeland Security*

United States
Secret Service

Other

- Category serves as catch all group for newly identified exploits that do not fit in previously listed categories
- Penetration Testing
- Innovative ways to attack a system
- Zero-day Exploits



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 4 – Predicting the Nature and Location of Intrusion Artifacts

- Predicting the Nature and Location of Intrusion Artifacts
- Relating Observed Events to Network Services and Traffic Types
- Mapping Observed Activity to Traffic Flow
- Using Traffic Flow and Service Type to Predict Artifact Location



*U.S. Department of
Homeland Security*

United States
Secret Service

Finding Intrusion Artifacts

- Mapping observed events to related applications and traffic
- Map observed activity to traffic flow of network traffic
- Using probable traffic flow, applications involved and traffic types, determine devices that may house artifacts of observed and hypothesized events
- Establish plan for gathering data from identified devices, and for identifying relevant artifacts within those data sets



*U.S. Department of
Homeland Security*

United States
Secret Service

Relating Events to Applications

- Correlate observed events to applications involved
- Help to locate potential artifacts
- For instance, if event was buffer overflow IDS alert, destination port of 80, could surmise target application may be Web server
- Recognizing this, place this application on your list of potential artifact sources, gather and analyze logs from that application



*U.S. Department of
Homeland Security*

United States
Secret Service

Relating Events to Applications

- Identify network traffic types that correspond to observed TCP/UDP ports
- For instance, observed TCP port 25 traffic indicates SMTP most likely involved
- Identify applications related to observed and/or extrapolated network traffic types
- From example, if SMTP were likely protocol, indicative that an e-mail server and client application probably also involved



*U.S. Department of
Homeland Security*

United States
Secret Service

Concept of Profiling an Event

```
Mar  1 14:24:53 bastion snort: [1:648:7] SHELLCODE x86 NOOP [Classification:  
Executable code was detected] [Priority: 1]: {TCP} 4.152.207.238:4771 ->  
11.11.79.90:80
```

Profile of Observed Activity

Port 80

Related Protocol: HTTP

Related Applications:

- Web Browser
- Web Server



*U.S. Department of
Homeland Security*

United States
Secret Service

Additional Applications

- Identify applications that have capability of logging activity related to network traffic types
- Applications you have singled out
- For instance, SMTP gateways would have capability of logging data about traffic between e-mail servers and clients



*U.S. Department of
Homeland Security*

United States
Secret Service

Additional Applications

- Identify applications directly involved in generation of observed events
- Includes security devices/applications that produced log files that contained initial observations
- Following example from previous slides, Snort IDS that generated alert would be added to list of applications that may contain relevant artifacts



*U.S. Department of
Homeland Security*

United States
Secret Service

Identifying Additional Applications

```
Mar  1 14:24:53 bastion snort: [1:648:7] SHELLCODE x86 NOOP [Classification:  
Executable code was detected] [Priority: 1]: {TCP} 4.152.207.238:4771 ->  
11.11.79.90:80
```

Profile of Observed Activity

Port 80

Related Protocol: HTTP

Related Applications:

- Web Browser
- Web Server
- **Snort IDS**



*U.S. Department of
Homeland Security*

United States
Secret Service

Recording Traffic Types

- Locate all devices that related traffic may have passed through
- For instance, if investigator believes that intrusion-related traffic passed through specific point of ingress/egress for network, devices at that point (firewalls, routers, IDS sensors, etc.) could potentially contain important artifacts



*U.S. Department of
Homeland Security*

United States
Secret Service

Mapping Activity to Network Traffic

- Obtain a logical or physical network diagram, and/or access to a network administrator that has working knowledge of current topology
- Diagram should be broad enough to include all points of ingress/egress from affected network segments, including paths to Internet
- Ascertain IP addresses for devices involved in incident
- Identify ports and protocols corresponding to related network protocols



*U.S. Department of
Homeland Security*

United States
Secret Service

Mapping Activity to Network Traffic

- Use information obtained to identify all routes between affected devices and between those devices and Internet
- Record routes in notes or mark on working copies of any network diagrams



*U.S. Department of
Homeland Security*

United States
Secret Service

Other Routes of Interest

- Alternate points of network traffic ingress/egress from network segment on which each device resides
- Identify routes to major service network segments not inline with default gateway
- Network segments with directory servers, e-mail servers, file and print servers, backup servers etc



*U.S. Department of
Homeland Security*

United States
Secret Service

Other Routes of Interest

- Routes used by incoming traffic to affected network segment if not the same as default outbound route
- Routes used by public service requests to segment, internal service requests, VPN pathways, etc
- In network, check specific protocols sent through alternate routes to reach proxy servers
- If found, identify routes between affected network segment and those proxy servers



*U.S. Department of
Homeland Security*

United States
Secret Service

Adding Source and Destination

```
Mar  1 14:24:53 bastion snort: [1:648:7] SHELLCODE x86 NOOP [Classification:  
Executable code was detected] [Priority: 1]: {TCP} 4.152.207.238:4771 ->  
11.11.79.90:80
```

Profile of Observed Activity

Port 80

Related Protocol: HTTP

Related Applications:

- Web Browser
- Web Server
- Snort IDS

Source: 4.152.207.238

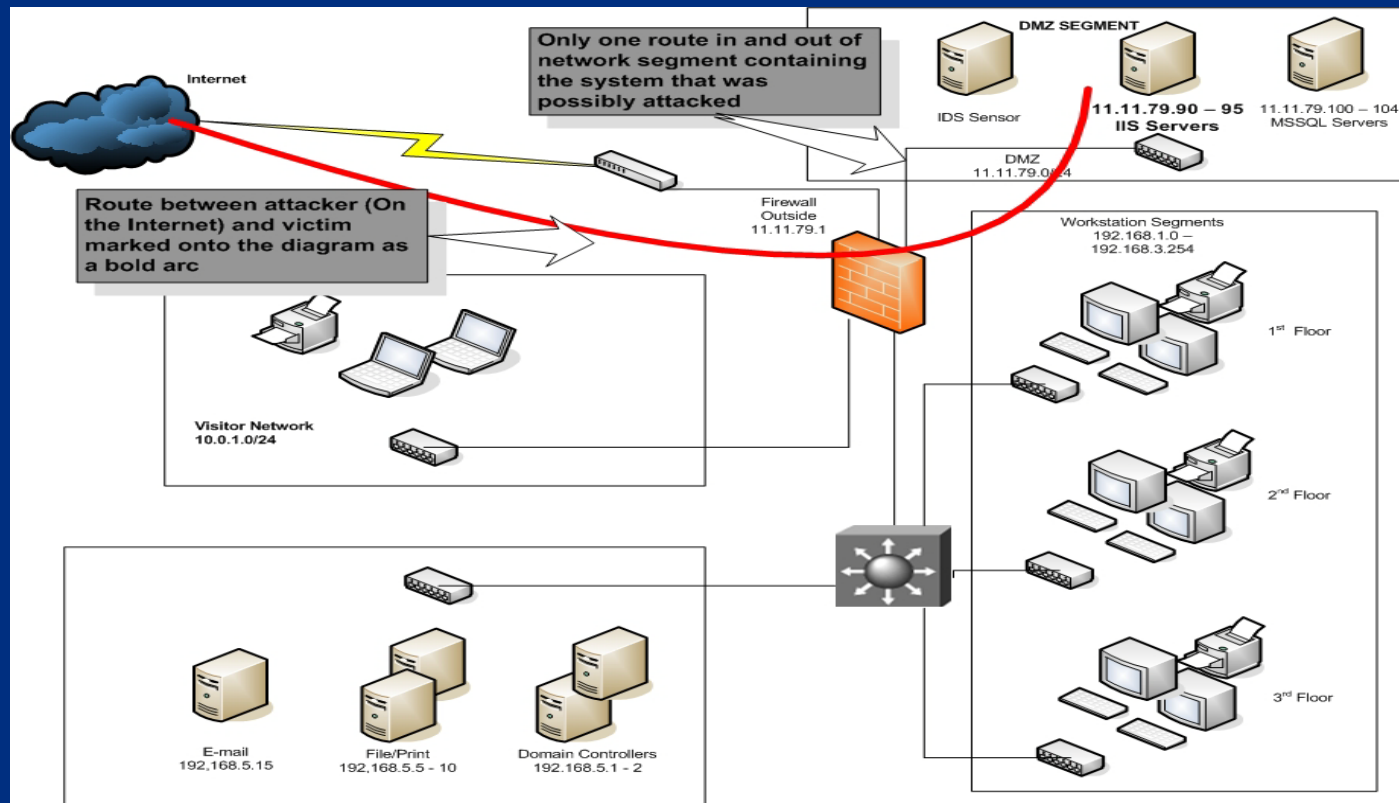
Destination: 11.11.79.90



*U.S. Department of
Homeland Security*

United States
Secret Service

Mapping Traffic Routes



U.S. Department of
Homeland Security

United States
Secret Service

Predicting Artifact Location: Devices

- Determine host system for application
- Determine if application uses local or remote (SAN, NAS, etc.) storage
- If remote is used, identify associated storage devices
- Determine if host system is backed up on a regular basis or and whether data backed up to local media, or remote system
- If local, where are tapes or other backup media stored
- If remote, identify remote backup server



*U.S. Department of
Homeland Security*

United States
Secret Service

Predicting Artifact Location: Devices

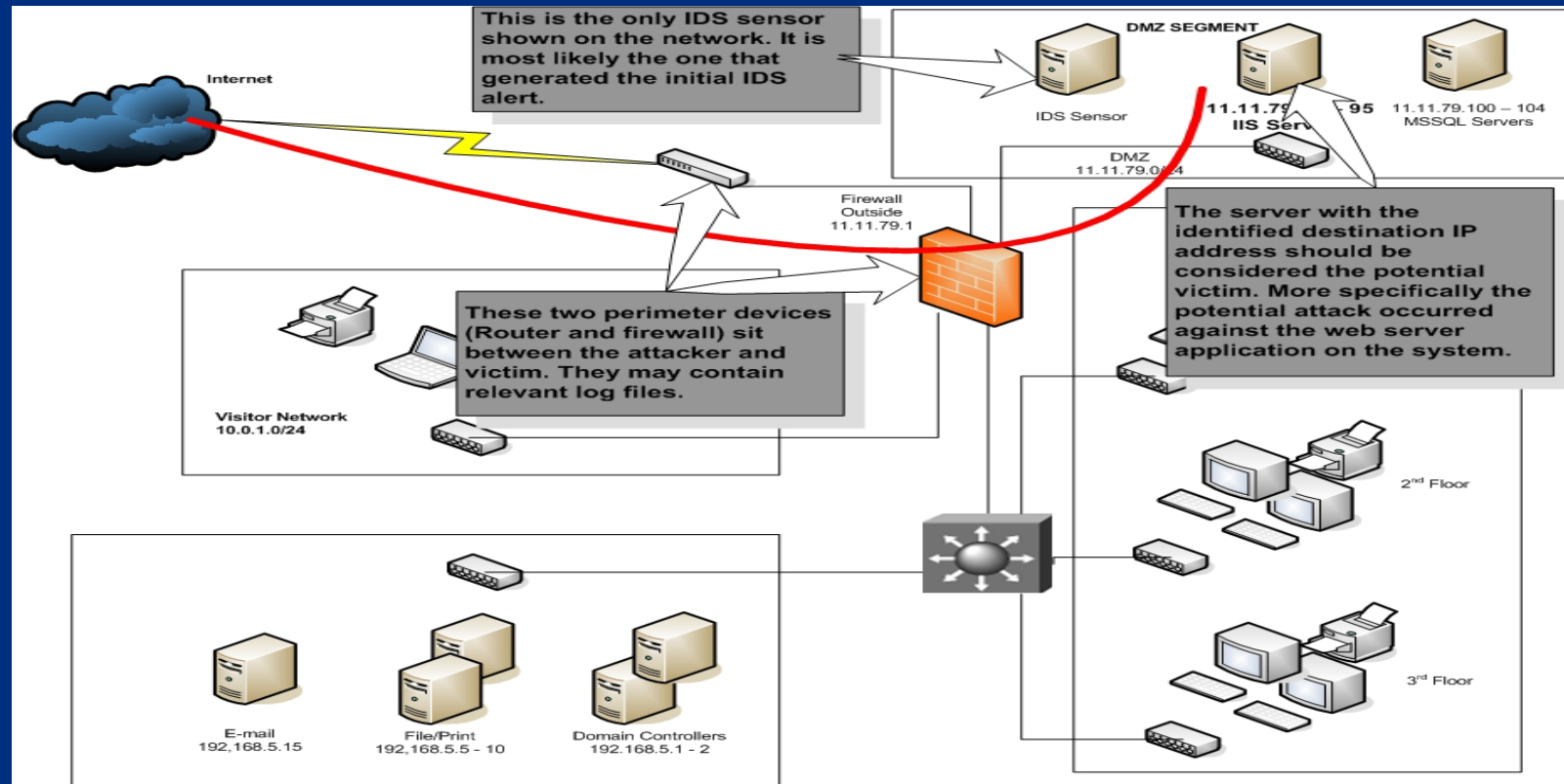
- Determine if application is part of distributed application system (such as a Web server with a database backend)
- Identify other applications in system, and hosts on which they reside
- If multiple systems host application as part of a load-balancing configuration, identify all systems hosting copies of application
- If application configured to use proxy device when communicating on network, identify all associated proxy devices



*U.S. Department of
Homeland Security*

United States
Secret Service

Predicting Artifact Location: Devices



U.S. Department of
Homeland Security

United States
Secret Service

Predicting Artifact Location: Files

- If application keep logs determine full path to log storage location
- If application or host system configured to send logs to remote repository, identify system
- Determine full path and name of files in which application stores configuration information



*U.S. Department of
Homeland Security*

United States
Secret Service

Predicting Artifact Location: Files

- Determine name and full path of files in which application stores persistent and temporary data
- Determine whether application requires authentication
- Determine if application uses its own authentication mechanism or forward authentication data to an outside application (such as Active Directory)



*U.S. Department of
Homeland Security*

United States
Secret Service

Predicting Artifact Location: Files

- Following example scenario, potential victim in attack could be an IIS Web server that contains certain log files to be analyzed
- Windows Event log
- IIS log
- Dr. Watson log



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 5 – Using Log Analysis to Evaluate an Intrusion Hypothesis

- Hypothesis Evaluation
- Acquiring Target Log Files
- Reviewing Target Log Formats
- Establishing Search/Extraction Criteria
- Searching Target Logs and Extracting Relevant Data
- Recording and Correlating Findings
- Keeping Track of New Leads



*U.S. Department of
Homeland Security*

United States
Secret Service

Hypothesis Evaluation

- Acquire target log files
- Review the format of collected logs
- Establish search/extraction criteria based upon predicted artifacts and log format
- Search log files and extract relevant data
- Record and correlate findings
- Document unexpected findings related to case (“leads”)



*U.S. Department of
Homeland Security*

United States
Secret Service

Procedure Selection

- Procedure can locate specific potential artifacts identified in previous step in Scientific Method
- Procedure should have been tested and peer reviewed
- Procedure should be repeatable
- Procedure should be as objective as possible



*U.S. Department of
Homeland Security*

United States
Secret Service

Acquiring Log Files

- Log files may be provided directly by incident responder or network administrator who collected them from original source media
- Could obtain physical or logical image of original storage media containing log files, and extract logs from image
- Could obtain logical copy log files from source system or device
- Regardless of method, ensure logs collected in sound manner in accordance with maintaining integrity of evidence



*U.S. Department of
Homeland Security*

United States
Secret Service

Previewing Log Formats

- Before analyzing, preview format to ensure you know how to read them properly and use correct methods for searching
- Search techniques significantly different between text and binary logs
- Information may be presented in different forms in text logs
- Fields and format may differ and record separators
- For example, time may be represented in 24-hour format or 12-hour with AM or PM specified



*U.S. Department of
Homeland Security*

United States
Secret Service

Determining File Type

- View file extension and correlate to file type
- For instance, file with “.EVT” extension is Windows Event Log file and should be viewed with Microsoft Event Viewer application
- If unfamiliar with extension, research it online
- Use GNU “file” command, does not rely on file extensions, useful if log file does not include extension



*U.S. Department of
Homeland Security*

United States
Secret Service

Determining File Type

- Attempt to view file with text log viewer, such as notepad.exe, or GNU command such as “cat”, “more”, “tail”, etc
- If successful, file is text log and viewable as such
- File – Open dialog in Wireshark will display format of binary capture files that it recognizes when file is highlighted



*U.S. Department of
Homeland Security*

United States
Secret Service

Determining Data Format

- Determine if records include one line or multiple lines
- Identify field and record separators
- Determine where common data types (IP addresses, port numbers, date/time, etc.) are located in each record, if anywhere
- Determine if locations are always same or vary



*U.S. Department of
Homeland Security*

United States
Secret Service

Search/Extraction Criteria

- Known or estimated time frame
- Observed or predicted source or destination IP addresses
- Messages that correlate with observed or predicted activity
- Observed user name or alias
- Observed or predicted network protocols or traffic types
- Any combination of criteria mentioned in items above



*U.S. Department of
Homeland Security*

United States
Secret Service

Search/Extraction Criteria

- Previously listed criteria examples are guides only
- No hard and fast rule for choosing specific search and extraction criteria
- Criteria must be selected based upon potential for producing data to further investigation of hypothesis



*U.S. Department of
Homeland Security*

United States
Secret Service

Correlation: Timeline Unification

- Normalize all log files to synchronized time and time notation
- Involves changing actual date/time stamps in log file, should only be performed on working copies of log
- Record events identified during initial observation and subsequent testing/evaluation into single timeline
- Adjust time on each event as necessary as recorded



*U.S. Department of
Homeland Security*

United States
Secret Service

Correlation: Event Verification

- Any event can be correlated with data in full network traffic capture
- Verify Web browser history with proxy server logs, both record URL access and associated times
- Verify IDS scan alerts with firewall logs
- Verify IDS password attacks alerts with authentication logs
- Verify e-mail header date/time stamps with e-mail gateway or e-mail server logs



*U.S. Department of
Homeland Security*

United States
Secret Service

Correlation: Synchronize Times

- Compare dates/times for events against multiple sources to see if there are discrepancies in time in data sources
- For instance, user IE history shows access to Web mail occurring at 2105, Web proxy shows access occurred at 2135
- Analyst could use two events to determine that proxy server was most likely set 30 minutes behind clock on subject system
- Ideally, multiple events correlate to verify time



*U.S. Department of
Homeland Security*

United States
Secret Service

Correlation: Synchronize Times

- Compare date/time stamps embedded in files with file system date/time stamps
- Compare date/time stamp of last entry in log with file system last accessed time
- If event involved access to one or more files, check appropriate file system date/time stamps for file



*U.S. Department of
Homeland Security*

United States
Secret Service

Unexpected Findings

- May often discover information not directly predicted during initial analysis of hypothesis
- Can be identified as a “lead”
- Information is sometimes related to hypothesis, and other times important but outside of current investigation
- Information should be recorded for follow up as needed



*U.S. Department of
Homeland Security*

United States
Secret Service

Lead Tracking

- New leads should be documented
- Leads should be recorded in Attribute List spreadsheet along with other relevant data
- Entries representing leads should be marked as to whether or not they are relevant to current working hypothesis
- Highlight other leads in a different color
- List other lead entries on a separate page, tab, table, etc.
- Use a column in a table to mark other lead entries as such



*U.S. Department of
Homeland Security*

United States
Secret Service



*U.S. Department of
Homeland Security*

United States
Secret Service

Module 13 – Log Sources



*U.S. Department of
Homeland Security*

United States
Secret Service

You Will Learn . . .

- Windows Log Sources
- Linux Log Sources
- Solaris Log Sources
- Log Searching
- IDS Logs



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 1 – Windows Log Sources

- Windows Logs
- Windows Services Logs



*U.S. Department of
Homeland Security*

United States
Secret Service

Windows Logs

- Windows includes Outlook or Outlook Express as a mail client
- Default location for log files in Windows 2000, Server 2003 and XP is individual user's profile
- Outlook's MAPI accounts log found at: C:\Documents and Settings\username\Local Settings\Temp\Opmllog.log
- If user established Hotmail account in Outlook, events logged in: C:\Documents and Settings\username\Local Settings\Temp\Outlook Logging\Hotmail\http0.log



*U.S. Department of
Homeland Security*

United States
Secret Service

Microsoft SQL Databases

- One of most popular database services used in businesses
- Stores log files in C:\MSSQL\LOG



*U.S. Department of
Homeland Security*

United States
Secret Service

Log files in MSSQL\LOG

- ERRORLOG – MS SQL's default error log file
 - If logging configured to create new files on routine basis, or file grows too large, additional error logs will be created with a sequential number appended
- SQLAGENT.OUT – Can contain information generated by SQL programmer or messages generated by default in administrative panel
 - Files can have numbers for versions at end
 - File with OUT suffix is current log



*U.S. Department of
Homeland Security*

United States
Secret Service

Log files in MSSQL\LOG

- SQLDump9999.txt and SQLDump9999.mdmp – Special dump files generated if SQL Server crashes or terminates unexpectedly
 - Information in files generally contains memory and data pointers at time of failure
 - Also possible for administrator, or attacker to force generation of these files under special circumstances
- NOTE: If server running, may not be possible to copy or open current log files



*U.S. Department of
Homeland Security*

United States
Secret Service

MySQL

- MySQL is free, open source database application, popular on many Windows systems
- Default location for installation of MySQL in Windows is C:\Program Files\MySQL\MySQL Server X.X
- In folder name, X.X is software's version number



*U.S. Department of
Homeland Security*

United States
Secret Service

Directories and Logs in X.X Folder

- Bin
 - Contains client programs and server program
- Data
 - Holds log files and actual databases
- Share
 - Has error message files
- Error filename will typically start with network host name of system MySQL is running on and end with .err suffix



*U.S. Department of
Homeland Security*

United States
Secret Service

Microsoft Access

- Errors generated by Access stored in Windows Event logs
- Information for retrieval of Event logs discussed with System Logs



*U.S. Department of
Homeland Security*

United States
Secret Service

Internet Information Server (IIS)

- IIS is service used by millions of Windows based servers to host web, FTP, and e-mail services
- Depending on version in use, logs can be found in different locations
- IIS normally stores logs in default folder,
- Log location can be easily changed in administration control panel



*U.S. Department of
Homeland Security*

United States
Secret Service

Internet Information Server (IIS)

- Log files stored in C:\winnt\system32\logfiles for IIS versions 4 and 5, found on Windows NT 4.0 and Windows 2000
- Log files stored in: C:\windows\system32\logfiles for IIS version 6 and 7, found on Windows XP and newer systems



*U.S. Department of
Homeland Security*

United States
Secret Service

Internet Information Server (IIS)

- Log files named “W3SVC” followed by Site Instance ID, numbered sequentially for each service
 - For example, first web site log files start with W3SVC1, and second W3SVC2
- Web enabled service originate in IIS service
- FTP and DNS messages will be mingled in same W3SVC file if services are active



*U.S. Department of
Homeland Security*

United States
Secret Service

Windows System Logs

- Almost all other services that originate in Windows log entries into one or all standard Event Logs
- Logs divided into Application, Security and System
- Use Event Viewer to view logs
- Log files stored in a mixed binary format, making standard text based tools ineffective



*U.S. Department of
Homeland Security*

United States
Secret Service

Windows System Logs

- Can choose log file of interest from menu in Event Viewer and export as:
 - Tab Delimited text
 - Comma Delimited text
 - Tab Delimited Unicode text
 - Comma Delimited Unicode text
- Exported files can be filtered and searched using tools like Grep and Findstr



*U.S. Department of
Homeland Security*

United States
Secret Service

Directory Services

- If Directory Services is configured, applicable events found under Directory Services in Event Viewer



*U.S. Department of
Homeland Security*

United States
Secret Service

Remote Logs

- Looking at mounted share locations and names, may give indication that logs are stored remotely
- Examination of remote shares may provide folder and file names which indicate what types of logs are stored remotely



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 2 – Linux Log Sources

- Linux Logs



*U.S. Department of
Homeland Security*

United States
Secret Service

Linux Mail Logs

- Linux is based on Unix style kernel
- Mail services provided by sendmail processes
- Logs for these services usually found in `/var/log/maillog`



*U.S. Department of
Homeland Security*

United States
Secret Service

Database

- MySQL is most popular database program within Linux community
- MySQL logs typically found in `/var/log/mysqld.log`



*U.S. Department of
Homeland Security*

United States
Secret Service

Linux Services Files

- `/var/log/message`: General messages and system related errors
- `/var/log/auth.log`: Remote Login Authentication logs
- `/var/log/secure`: Remote Login Authentication log
- `/var/log/kern.log`: Kernel logs
- `/var/log/cron.log`: Crond logs, for services that start automatically



*U.S. Department of
Homeland Security*

United States
Secret Service

Linux Services Files

- `/var/log/httpd/`: Apache web server access and error logs directory
- `/var/log/boot.log` : System boot log
- `/var/log/utmp` or `/var/log/wtmp` : Binary Login history file
- `/var/log/yum.log`: Yum log files to track installed and uninstalled applications



*U.S. Department of
Homeland Security*

United States
Secret Service

Linux Directory Management

- Linux does not directly support Microsoft Active Directory
- Numerous third party add-on tools available to provide the service
- Seek documentation for specific AD tool encountered and determine location of logs for each



*U.S. Department of
Homeland Security*

United States
Secret Service

Linux System Logs

- Most located in the `/var/log/message` file



*U.S. Department of
Homeland Security*

United States
Secret Service

Remote Logs

- Looking at mounted share locations and names may provide indication that logs are stored remotely
- Examination of remote shares may identify folder and file names which indicate what types of logs are stored remotely



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 3 – Solaris Log Sources

- Solaris Logs



*U.S. Department of
Homeland Security*

United States
Secret Service

Solaris Mail

- Depending on version of Solaris, may find file in /etc directory called syslog.conf, and location of sendmail logs listed inside
- Many ISP's moved to custom mail software
- Seek documentation on software to determine log file location



*U.S. Department of
Homeland Security*

United States
Secret Service

Databases

- If MySQL installed on Solaris system, look for logs in default locations of /usr/local/mysql/data or /opt/mysql/mysql/data
- Oracle is popular database for Solaris systems
- Determine version and release level of Oracle software
- Search for default installation location of log files



*U.S. Department of
Homeland Security*

United States
Secret Service

Solaris Services

- Most Solaris services put log messages in `/var/adm/messages` log file
 - General catch all file for log entries in Solaris



*U.S. Department of
Homeland Security*

United States
Secret Service

Directory Management

- Solaris doesn't natively support Microsoft Active Directory directly
- Numerous third party add-on tools available to provide this service
- Seek out documentation for specific AD tool and determine location of logs for each



*U.S. Department of
Homeland Security*

United States
Secret Service

Solaris System

- Solaris system log files located in /var directory
- Usually several nested directories of log files under /var directory
- Investigation may show some or all have information of evidentiary value
- Cannot open files in use



*U.S. Department of
Homeland Security*

United States
Secret Service

Remote Logs

- Search for pipes and hard links to mounted volumes in order to discover whether logs are stored remotely
- In Solaris environment attempt to locate a certified Solaris administrator to discover obfuscated links



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 4 – Log Searching

- Log Searching
- Regular Expressions



*U.S. Department of
Homeland Security*

United States
Secret Service

Log Searching

- Flexibility is important feature for tool used to search through log files
- Wide variety of log files
- Require search for different types of values
- Tools and techniques must be usable regardless of log type and search values



*U.S. Department of
Homeland Security*

United States
Secret Service

GREP

- GREP (Global Regular Expressions Print)
- Newer version EGREP (The E stands for “Extended”)
- Primary applications used for searching and filtering text logs
- Use regular expressions to define search parameters
- Used because regular expressions are most common method for defining search parameters, and used in many other applications, such as PERL, Snort, and EnCase



*U.S. Department of
Homeland Security*

United States
Secret Service

GREP

- GREP typically found in Unix, Linux, and OS X environments
- Versions available for Windows operating systems



*U.S. Department of
Homeland Security*

United States
Secret Service

Findstr

- Windows does not natively ship with GREP
- Does include Findstr, similar command line utility to find specific strings of text in log file or other type text file
- Typing “findstr /?” at command prompt displays quick help screen of options and command format



*U.S. Department of
Homeland Security*

United States
Secret Service

Findstr Options

- /I to disable case sensitivity
- /S to search all files in current directory and subdirectories
- /R to allow use of regular expressions
- /N to print line numbers
- /G:filename to use a file of key strings to search for



*U.S. Department of
Homeland Security*

United States
Secret Service

Regular Expressions

- Patterns used for executing searches and filters
- Accomplished by combining literal text and special characters, called metacharacters, to create a pattern used to search files



*U.S. Department of
Homeland Security*

United States
Secret Service

Examples of Set Pattern Items

- IP addresses
- Dates and time
- Phone numbers
- URLs
- Credit card numbers
- Social Security numbers



*U.S. Department of
Homeland Security*

United States
Secret Service

Regular Expressions

- Should understand regular expressions and how to use them effectively to search or filter text logs
- Many tools incorporate regular expression engines into functionality
- Some GNU command line tools, such as grep/egrep, sed and awk, and many text editors, allow searching and/or replacement of text through use of regular expressions
- Regular Expression engines and syntax may vary slightly from product to product



*U.S. Department of
Homeland Security*

United States
Secret Service

Literal Character Searches

- Simplest type of regular expression is literal representation of target value
- For example, search for “jsmith” in log.txt by simply telling egrep to search for string “jsmith”

[prompt]# egrep “jsmith” log.txt

- Most programs search files one line at a time
- Command line above will return each line in file that contains string “jsmith” to whatever output is specified



*U.S. Department of
Homeland Security*

United States
Secret Service

Regular Expression Example

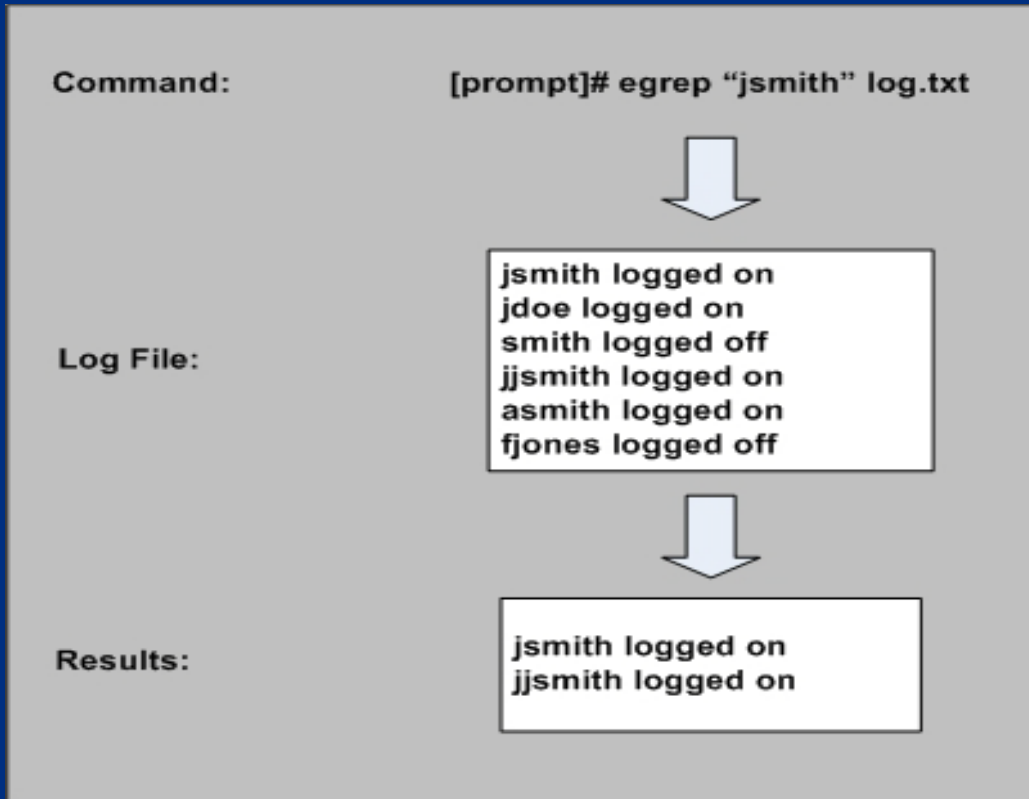
- Example of a search for a literal string is shown on next slide
- Log file searched for string “jsmith” using egrep
- Notice, any line that included “jsmith” was matched, even one that begins with “jjsmith”
- It does not matter what is before or after target string, only that it exists
- “jsmith” could be a stand-alone string, or part of a string such as “jsmithsonian”



*U.S. Department of
Homeland Security*

United States
Secret Service

Regular Expression Example



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 5 – IDS Logs

- IDS Logs



*U.S. Department of
Homeland Security*

United States
Secret Service

Intrusion Detection Systems

- Intrusion Detection Systems (IDS), prolific, found in many networked environments
- Probably find most logs generated by these systems are binary rather than text
- When files encountered, may require use of proprietary program to view or convert files to text
- Some save logs in libpcap format, can use packet sniffer tools like Wireshark to open, view and export



*U.S. Department of
Homeland Security*

United States
Secret Service

Snort

- Popular IDS and intrusion reporting tool
- Free application, allows administrators to flag alerts, on both live and captured traffic
- After parsing traffic, will generate text log displaying alerts of suspicious traffic encountered
- Requires complex set of steps to configure, and configuration will change with each type of log or capture
- By default, Snort's log files on Linux, Unix, or OS X system, found in /var/log/snort



*U.S. Department of
Homeland Security*

United States
Secret Service



*U.S. Department of
Homeland Security*

United States
Secret Service

Module 14 – Log Analysis



*U.S. Department of
Homeland Security*

United States
Secret Service

You Will Learn . . .

- Binary Traffic Analysis
- Manual Log Analysis
- Automated Log Analysis Tools



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 1 – Binary Traffic Analysis

- Introduction to Wireshark
- Converting Binary Logs to Text Format
- Filtering and Searching in Wireshark
- Colorizing Data Using Filters in Wireshark
- Generating Statistics with Wireshark
- Exporting Data from Wireshark



*U.S. Department of
Homeland Security*

United States
Secret Service

Wireshark

- Powerful open source protocol analyzer
- Opens a variety of binary log formats
- Act as a sniffer
- Translates, decodes, known protocols from binary to human readable format
- Displays highly detailed information on frame-by-frame basis
- Provides search of capture log for frames that match specific criteria
- Automatically reconstruct TCP sessions



*U.S. Department of
Homeland Security*

United States
Secret Service

Procedure: Importing Logs into Wireshark

- This is a Step / Action exercise in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

Viewing Binary Logs in Wireshark

- Top Pane: Summary of captured frames, including frame number, date and time, source IP, destination IP, protocol and basic description
- Middle Pane: Decoded protocol header information, organized inversely to order of each protocol within OSI model
- Bottom Pane: Full frame contents in hexadecimal on left side with any included clear text displayed on right



*U.S. Department of
Homeland Security*

United States
Secret Service

Procedure: Creating a Filter with Wireshark

- This is a Step / Action exercise in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

Procedure: Creating a Color Filter with Wireshark

- This is a Step / Action exercise in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

Binary vs. Text Format

- More efficient at times to change binary logs to text format
- As text, logs can be manipulated using text log filtering techniques to quickly find target data
- Change binary logs to text format with tcpdump
- Default output of tcpdump is text format



*U.S. Department of
Homeland Security*

United States
Secret Service

Tcpdump Command

- **[prompt]# tcpdump -r log.cap > log.txt**
- Command directs tcpdump to read file log.cap, and place a text interpretation of contents into text file log.txt
- By default tcpdump does not print full contents of each packet, just summary data



*U.S. Department of
Homeland Security*

United States
Secret Service

Wireshark Binary Log Filtering

- Capture filters: Interface used to filter data while being captured from network; uses tcpdump syntax
- Display filters: Interface used to filter currently displayed traffic
- Color filters: Interface used to apply colors to certain packets based upon a filter expression
- Find menu: Standard find menu that allows packet to be searched by hex value or string, can also use to enter display filters



*U.S. Department of
Homeland Security*

United States
Secret Service

Procedure: Setting Up Capture Filter

- This is a Step / Action exercise in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

Procedure: Creating a Display Filter

- This is a Step / Action exercise in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

Creating a Display Filter

Options available for an individual protocol (In this case UDP)

Operation to be used in the filter (In this case "equals")

Specific value for which to filter (53 in this example)

List of protocols that can be used in filters (Seen here: UDP, UDPCAP, UMA)

Ethereal: Filter Expression

Field name

- UDP
 - udp.srcport - Source Port
 - udp.dstport - Destination Port
 - udp.port - Source or Destination Port
 - udp.length - Length
 - udp.checksum_bad - Bad Checksum
 - udp.checksum - Checksum
- UDPCAP
- UMA

Relation

- is present
- ==
- !=
- >
- <
- >=
- <=

Value (unsigned, 2 bytes)

53

Predefined values:

Range (offset:length)

OK Cancel



U.S. Department of
Homeland Security

United States
Secret Service

Creating Display Filter for Keyword

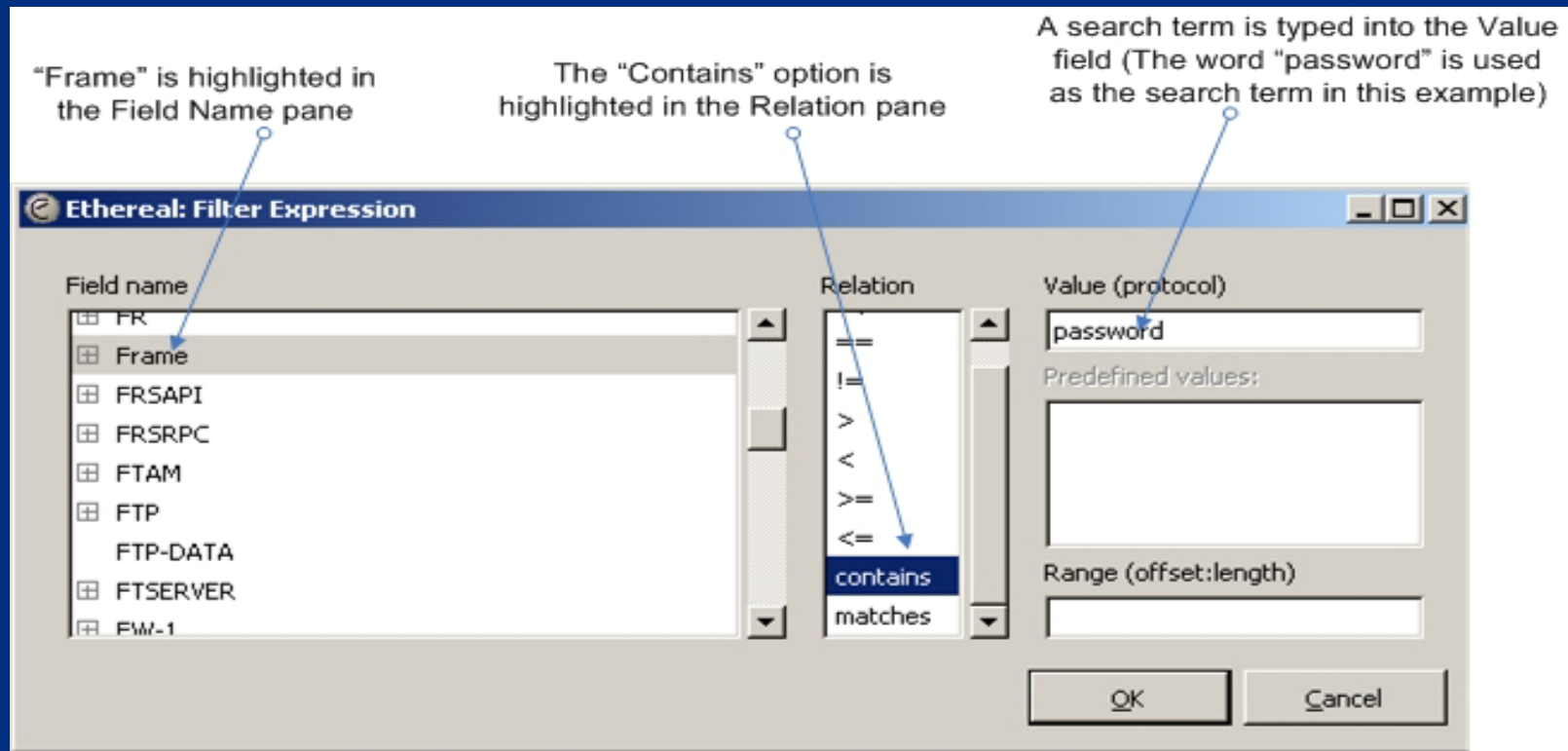
- Display filter can be created for a keyword
- Displays only packets that contain search term
- Done with “frame contains” display filter,
- Can be used to filter for presence of keyword anywhere in packet
- The “frame contains” filter can be found through normal display filter wizard



*U.S. Department of
Homeland Security*

United States
Secret Service

Display Filter for Keyword



U.S. Department of
Homeland Security

United States
Secret Service

Creating Hex Value Filter Display

- The “frame contains” expression syntax also used to filter for hexadecimal values
- Hex value is entered in place of keyword, colons used to separate value into pairs



*U.S. Department of
Homeland Security*

United States
Secret Service

Entering Display Filter Expressions

- When filter expression created using Display Filter wizard, text for filter entered in Display Filter field in main window
- Filter expressions can be entered directly as text into field instead of using wizard
- When entering display filter, if filter has valid syntax, background color of display filter field will be green, if not valid it will be red



*U.S. Department of
Homeland Security*

United States
Secret Service

Valid Display Filter

A filter expression for all traffic to or from the IP address 10.12.16.105

Display Filter field

The screenshot shows the Wireshark network protocol analyzer interface. The title bar reads "flash.cap - Ethereal". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. The toolbar contains various icons for file operations and analysis. The "Filter:" field is highlighted in green and contains the expression "ip.addr == 10.12.16.105". Below the filter field is a table of captured packets. The table has five columns: No., Time, Source, Destination, and Protocol. The first four packets are visible, all showing traffic to or from the IP address 10.12.16.105.

No. -	Time	Source	Destination	Protocol
2	0.468711	10.12.16.105	146.82.218.135	TCP
3	0.486239	146.82.218.135	10.12.16.105	TCP
4	0.486269	10.12.16.105	146.82.218.135	TCP
5	0.486400	10.12.16.105	146.82.218.135	HTTP



U.S. Department of
Homeland Security

United States
Secret Service

Display Filter Syntax

- See student book for examples of display filter syntax to include altering and combining filters.



*U.S. Department of
Homeland Security*

United States
Secret Service

Procedure: Creating Color Filters

- This is a Step / Action exercise in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

Procedure: Searching in Wireshark

- This is a Step / Action exercise in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

Wireshark Statistics Menu

- “Statistics” menu in the menu bar for generating various statistics about log data



*U.S. Department of
Homeland Security*

United States
Secret Service

Endpoints List

- In the Statistics menu, provides lists of statistics that revolve around addresses and TCP/UDP ports
- Separate window displays statistics
- Useful to see what IP addresses and ports are in a given binary capture



*U.S. Department of
Homeland Security*

United States
Secret Service

Endpoints Window

The screenshot shows a window titled "Endpoints: smb4-image.cap". It has a tabbed interface with tabs for various protocols: Ethernet: 15, Fibre Channel, FDDI, IPv4: 7, IPX, JXTA, TCP: 3, Token Ring, UDP: 7, WLAN, and RSVP. The "TCP: 3" tab is selected, displaying a table of TCP endpoints. Below the table is a "Copy" button. At the bottom left, there is a checkbox labeled "Name resolution" which is checked, and a "Close" button.

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
10.76.23.88	139	172	50701	86	32910	86	17791
10.7.20.233	1539	165	50223	82	17495	83	32728
10.7.20.233	1538	7	478	4	296	3	182

Tabs can be selected to change the statistics displayed by the window. This example shows stats based upon TCP ports. There is one line per unique TCP port seen in this log.

Grey text in a tab means that the element presented by that tab was not present in the log. For instance in this example, there were no IPX addresses, so that tab is not available.

The Copy button can be used to copy the contents of whatever tab is being displayed to a text file in comma delimited format.

This box is checked by default. Leaving it selected will cause Ethereal to attempt to resolve addresses to names. For instance it may try to resolve an IP address to a NetBIOS name.



U.S. Department of
Homeland Security

United States
Secret Service

Protocol Hierarchy Statistics

- Option in Statistics menu, provides a list of protocols that were seen in a given capture, and volumes of protocol activity
- May be possible to determine applications being used on network from this information and provide snapshot of activity
- Wireshark does not recognize all protocols, and may miss a protocol used over a non-standard port



*U.S. Department of
Homeland Security*

United States
Secret Service

Protocol Hierarchy Statistics

Ethereal: Protocol Hierarchy Statistics

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00%	210	53963	0.020	0	0	0.000
[-] Ethernet	100.00%	210	53963	0.020	0	0	0.000
Address Resolution Protocol	13.33%	28	1662	0.001	28	1662	0.001
[-] Internet Protocol	85.24%	179	51804	0.020	0	0	0.000
[-] User Datagram Protocol	3.33%	7	1103	0.000	0	0	0.000
[-] NetBIOS Datagram Service	1.43%	3	735	0.000	0	0	0.000
[-] SMB (Server Message Block Protocol)	1.43%	3	735	0.000	0	0	0.000
[-] SMB MailSlot Protocol	1.43%	3	735	0.000	0	0	0.000
Microsoft Windows Browser Protocol	1.43%	3	735	0.000	3	735	0.000
NetBIOS Name Service	1.90%	4	368	0.000	4	368	0.000
[-] Transmission Control Protocol	81.90%	172	50701	0.019	45	22968	0.009
[-] NetBIOS Session Service	60.48%	127	27733	0.011	4	372	0.000
SMB (Server Message Block Protocol)	58.57%	123	27361	0.010	116	18145	0.007
[-] LogicalLink Control	1.43%	3	497	0.000	0	0	0.000
Dynamic Trunking Protocol	0.95%	2	120	0.000	2	120	0.000
Cisco Discovery Protocol	0.48%	1	377	0.000	1	377	0.000

Hierarchy of protocols seen in the binary capture. The box by each protocol name can be expanded or contracted to change the view.

The "%Packets", "Packets" and "Bytes" columns indicate the levels of activity seen by each protocol listed.



U.S. Department of
Homeland Security

United States
Secret Service

Conversations List

- “Conversations” option in Statistics menu offers lists of source/destination address combinations
- Wireshark presents source and destination address combinations communicating in capture, and number of packets between each pair
- Packet volume is shown for each direction of communication between pair



*U.S. Department of
Homeland Security*

United States
Secret Service

Conversations Window

Address A	Address B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B
10.12.16.105	216.239.39.99	4	234	1	54	3	180
10.12.16.101	10.12.16.105	28	6106	13	2125	15	3981
10.12.16.105	63.236.111.50	33	5446	18	3015	15	2431
10.12.16.105	146.82.218.135	2790	2829604	942	55630	1848	2773974

Tabs can be selected to change the statistics displayed by the window. This example shows stats based upon IP address source and destination combinations are shown.

Grey text in a tab means that the element presented by that tab was not present in the log. For instance in this example, there were no IPX addresses, so that tab is not available.

The Copy button can be used to copy the contents of whatever tab is being displayed to a text file in comma delimited format.

This box is checked by default. Leaving it selected will cause Ethereal to attempt to resolve addresses to names. For instance it may try to resolve an IP address to a NetBIOS name.



U.S. Department of
Homeland Security

United States
Secret Service

HTTP Requests Stats Tree

- Wireshark can create custom list of HTTP get requests based upon specified display filter
- For example, a display filter for a specific IP address, shows all get requests for that IP
- Creating this statistic requires several steps
- See student book for HTTP Requests example and steps



*U.S. Department of
Homeland Security*

United States
Secret Service

Exporting Statistics

- Send copy of any generated statistics to file
- Option within some Wireshark statistics windows
- Statistics windows capable of exporting data will have “Copy” button on window



*U.S. Department of
Homeland Security*

United States
Secret Service

Exporting Statistics

Conversations: gmail2.cap

Ethernet: 2 | Raw Channel | EDD | **IPv4: 5** | IPX | ICMP | SCTP | TCP: 7 | Token Ring | UDP: 1 | WLAN | NCP | RSVP

IPv4 Conversations

Address A	Address B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B
10.12.16.103	20.1.6.9	7	1250	4	300	3
10.12.16.103	64.233.171.107	11	2477	6	1137	5
10.12.16.103	64.233.161.147	47	17310	25	6198	22
10.12.16.103	64.233.171.83	53	16204	26	6984	27
10.12.16.103	64.233.171.18	232	154731	108	42680	124

Copy

☒ Name resolution

Close



U.S. Department of
Homeland Security

United States
Secret Service

Exporting Statistics

- Pressing the copy button only puts the data into the copy buffer
- To save data, paste into a file
- Typical text file application such as Notepad will suffice
- Data should not be pasted directly into a spreadsheet because it will be placed into single cell
- Pasted data is in comma-delimited format, includes column headings
- Only tab currently displayed in statistic window is copied



*U.S. Department of
Homeland Security*

United States
Secret Service

Example Pasted Statistics

Address A,Address B,Packets,Bytes,Packets A->B,Bytes A->B,Packets A<-B,Bytes A<-B,
10.12.16.103,20.1.6.9,7,1250,4,300,3,950,
10.12.16.103,64.233.171.107,11,2477,6,1137,5,1340,
10.12.16.103,64.233.161.147,47,17310,25,6198,22,11112,
10.12.16.103,64.233.171.83,53,16204,26,6984,27,9220,
10.12.16.103,64.233.171.18,232,154731,108,42680,124,112051,



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 2 – Manual Log Analysis

- Filtering and Searching Text Logs
- Regular Expressions
- Deciding What to Search For
- Example Log



*U.S. Department of
Homeland Security*

United States
Secret Service

Filtering and Searching Text Logs

- Identify all log entries with a specific value or range of values
- Modify view of one or more log files based upon existence of an arbitrarily defined parameter



*U.S. Department of
Homeland Security*

United States
Secret Service

Filtering and Searching Toolset

- Flexibility is most important feature for tool used to perform filtering and searching
- Wide variety of log files encountered that will require search for different types of values
- Tools and techniques must be usable regardless of log type and value for which you are searching



*U.S. Department of
Homeland Security*

United States
Secret Service

Filtering and Searching Toolset

- GREP (Global Regular Expressions Print)
- Newer version EGREP (Extended Global Regular Expressions Print)
- Primary application used for searching and filtering text logs
- Use regular expressions to define search parameters
- Regular expressions are most common method for defining search parameters, used in other applications, such as PERL, Snort, and EnCase



*U.S. Department of
Homeland Security*

United States
Secret Service

Keywords

- Need a clear understanding of what you are searching for
- Rarely will 'shotgun' or broad focused search turn up useable data
- Decide on keywords that might be available in log file and might produce possible artifacts of intrusion



*U.S. Department of
Homeland Security*

United States
Secret Service

Sample Keywords for IIS Attack

- “Error” or “err”
- “Overflow”
- “Password” or “Pass”
- “Admin”
- “Unauthorized”
- IP addresses of interest



*U.S. Department of
Homeland Security*

United States
Secret Service

WordPad is Not Your Friend

- A tool like WordPad or Notepad can be used for these types of searches
- Data returned is not easily useable and does not allow filtering of information returned for clarity or further use
- Versions of Grep for Windows operating systems available from several sites
- GUI version, WinGrep, available at <http://www.wingrep.com>



*U.S. Department of
Homeland Security*

United States
Secret Service

Example Log

- Review the logs from an exploited web server on the next slide
- Logs are from the IIS server on the day of the attack
- Look at first few lines of log to determine program and version that created the file, and start and end dates of file
- Helpful to know approximate time attack occurred



*U.S. Department of
Homeland Security*

United States
Secret Service

Example Log

```
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2006-05-31 15:51:51
#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) sc-status sc-su
bstatus sc-win32-status
2006-05-31 15:51:51 W3SVC508294276 10.8.1.39 GET /index.html - 80 - 10.8.5.128 Mozilla/5.0+(Macintosh;+U;+PPC+Mac+OS+X+Mach-
0;+en-US;+rv:1.8.0.3)+Gecko/20060426+Firefox/1.5.0.3 200 0 0
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2006-05-31 19:58:31
#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) sc-status sc-su
bstatus sc-win32-status
2006-05-31 19:58:31 W3SVC508294276 10.8.1.39 GET / - 80 - 10.8.1.1 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+.
NET+CLR+1.1.4322) 403 14 5
2006-05-31 19:58:42 W3SVC508294276 10.8.1.39 GET /index.html - 80 - 10.8.1.1 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5
.1;+SV1;+.NET+CLR+1.1.4322) 200 0 0
2006-05-31 19:59:03 W3SVC508294276 10.8.1.39 GET /index.html/admin.pl - 80 - 10.8.1.1 Mozilla/4.0+(compatible;+MSIE+6.0;+Win
dows+NT+5.1;+SV1;+.NET+CLR+1.1.4322) 404 0 3
2006-05-31 19:59:05 W3SVC508294276 10.8.1.39 GET /index.html/backend.pl - 80 - 10.8.1.1 Mozilla/4.0+(compatible;+MSIE+6.0;+W
indows+NT+5.1;+SV1;+.NET+CLR+1.1.4322) 404 0 3
2006-05-31 19:59:05 W3SVC508294276 10.8.1.39 GET /index.html/backup.pl - 80 - 10.8.1.1 Mozilla/4.0+(compatible;+MSIE+6.0;+Wi
ndows+NT+5.1;+SV1;+.NET+CLR+1.1.4322) 404 0 3
2006-05-31 19:59:06 W3SVC508294276 10.8.1.39 GET /index.html/noteverthere.pl - 80 - 10.8.1.1 Mozilla/4.0+(compatible;+MSIE+6
.0;+Windows+NT+5.1;+SV1;+.NET+CLR+1.1.4322) 404 0 3
2006-05-31 19:59:06 W3SVC508294276 10.8.1.39 GET /index.html/cmd.pl - 80 - 10.8.1.1 Mozilla/4.0+(compatible;+MSIE+6.0;+Windo
ws+NT+5.1;+SV1;+.NET+CLR+1.1.4322) 404 0 3
```



*U.S. Department of
Homeland Security*

United States
Secret Service

IP Search

- Log is from attacked server, searching for server's IP address not useful since each entry should have the IP address
- If IP address of attacker is known, search for that
- In a NAT environment the IP could have been used or reused by another user in same log
- Better to save IP searches for later in order to search for specific IP and times together



*U.S. Department of
Homeland Security*

United States
Secret Service

String Search

- Attacker used an administrative account to log into server
- To do this, would have entered username and password
- Good starting point
- Using GREP, type: 'pass' IIS5211_6.txt
- Will search for string “pass” in every line of log file IIS5211_6.tx
- Result of such search on next slide



*U.S. Department of
Homeland Security*

United States
Secret Service

Searching for Password

```
2006-05-31 19:59:19 W3SVC508294276 10.8.1.39 GET /index.html/password.pl - 80 - 10.8.1.1 Mozilla/4.0+(com
2006-05-31 19:59:21 W3SVC508294276 10.8.1.39 GET /index.html/passwords.pl - 80 - 10.8.1.1 Mozilla/4.0+(co
2006-05-31 19:59:45 W3SVC508294276 10.8.1.39 GET /index.html/password.php - 80 - 10.8.1.1 Mozilla/4.0+(co
2006-05-31 19:59:46 W3SVC508294276 10.8.1.39 GET /index.html/passwords.php - 80 - 10.8.1.1 Mozilla/4.0+(c
2006-05-31 20:00:10 W3SVC508294276 10.8.1.39 GET /index.html/password.sh - 80 - 10.8.1.1 Mozilla/4.0+(com
2006-05-31 20:00:10 W3SVC508294276 10.8.1.39 GET /index.html/passwords.sh - 80 - 10.8.1.1 Mozilla/4.0+(co
2006-05-31 20:00:34 W3SVC508294276 10.8.1.39 GET /index.html/password.py - 80 - 10.8.1.1 Mozilla/4.0+(com
2006-05-31 20:00:36 W3SVC508294276 10.8.1.39 GET /index.html/passwords.py - 80 - 10.8.1.1 Mozilla/4.0+(co
2006-05-31 20:00:59 W3SVC508294276 10.8.1.39 GET /index.html/password.tgz - 80 - 10.8.1.1 Mozilla/4.0+(co
2006-05-31 20:01:01 W3SVC508294276 10.8.1.39 GET /index.html/passwords.tgz - 80 - 10.8.1.1 Mozilla/4.0+(c
2006-05-31 20:01:24 W3SVC508294276 10.8.1.39 GET /index.html/password.tar - 80 - 10.8.1.1 Mozilla/4.0+(co
2006-05-31 20:01:26 W3SVC508294276 10.8.1.39 GET /index.html/passwords.tar - 80 - 10.8.1.1 Mozilla/4.0+(c
2006-05-31 20:01:49 W3SVC508294276 10.8.1.39 GET /index.html/password.tar.gz - 80 - 10.8.1.1 Mozilla/4.0+
2006-05-31 20:01:51 W3SVC508294276 10.8.1.39 GET /index.html/passwords.tar.gz - 80 - 10.8.1.1 Mozilla/4.0
2006-05-31 20:02:15 W3SVC508294276 10.8.1.39 GET /index.html/password.asp - 80 - 10.8.1.1 Mozilla/4.0+(co
2006-05-31 20:02:15 W3SVC508294276 10.8.1.39 GET /index.html/passwords.asp - 80 - 10.8.1.1 Mozilla/4.0+(c
2006-05-31 20:02:40 W3SVC508294276 10.8.1.39 GET /index.html/password.aspx - 80 - 10.8.1.1 Mozilla/4.0+(c
2006-05-31 20:02:40 W3SVC508294276 10.8.1.39 GET /index.html/passwords.aspx - 80 - 10.8.1.1 Mozilla/4.0+(
2006-05-31 20:03:05 W3SVC508294276 10.8.1.39 GET /index.html/password.doc - 80 - 10.8.1.1 Mozilla/4.0+(co
2006-05-31 20:03:06 W3SVC508294276 10.8.1.39 GET /index.html/passwords.doc - 80 - 10.8.1.1 Mozilla/4.0+(c
2006-05-31 20:03:30 W3SVC508294276 10.8.1.39 GET /index.html/password.exe - 80 - 10.8.1.1 Mozilla/4.0+(co
2006-05-31 20:03:30 W3SVC508294276 10.8.1.39 GET /index.html/passwords.exe - 80 - 10.8.1.1 Mozilla/4.0+(c
2006-05-31 20:03:55 W3SVC508294276 10.8.1.39 GET /index.html/password.cmd - 80 - 10.8.1.1 Mozilla/4.0+(co
2006-05-31 20:03:56 W3SVC508294276 10.8.1.39 GET /index.html/passwords.cmd - 80 - 10.8.1.1 Mozilla/4.0+(c
```



*U.S. Department of
Homeland Security*

United States
Secret Service

Searching for Password

- Notice, on previous slide, a series of attempts to guess the password file for the system
- Not normal network traffic
- First clue of one method attempted by attacker
- Farther down the list is an attempt to get on the login page in admin directory
- The attacker is trying different account names and password combinations



*U.S. Department of
Homeland Security*

United States
Secret Service

Searching for Password

```
2006-05-31 20:46:09 W3SVC508294276 10.8.1.39 GET /admin/login.asp username=asdasd&password=asdasd 80 - 10.8.1.1 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+.NET+CLR+1.1.4322)
2006-05-31 20:47:39 W3SVC508294276 10.8.1.39 GET /admin/login.asp username=test&password=testpass 80 - 10.8.1.1 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+.NET+CLR+1.1.4322)
2006-05-31 20:49:52 W3SVC508294276 10.8.1.39 GET /admin/login.asp username=testFUZZCRTL&password=testpass 80 - 10.8.1.1 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+.NET+CLR+1.
2006-05-31 20:49:54 W3SVC508294276 10.8.1.39 GET /admin/login.asp username=testTo%20decrypt%20the%20distribution%20with%20key%20877895a%20742585e9%207607523e%2071a79000%2C%20enter&password=
```



*U.S. Department of
Homeland Security*

**United States
Secret Service**

Suspicious Text

- 2006-05-31 20:49:52 W3SVC508294276 10.8.1.39 GET /admin/login.asp username=testFUZZCTRL&password=testpass 80
- The text FUZZCTRL should appear suspicious
- Might be legitimate username or password or might not
- Search of Internet for FUZZCTRL finds reference to vulnerability scanning web proxy called Suru
- See examples of server attack that match lines shown



*U.S. Department of
Homeland Security*

United States
Secret Service

Response

- Now correlate known tool with IP address and time frame
- Allows you to now proceed with plan to contact ISP for domain that attacker is coming from
- Follow your agencies policy for contacting, serving preservation letters and obtaining warrants for information on attacker



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 3 - Automated Log Analysis Tools

- Sawmill



*U.S. Department of
Homeland Security*

United States
Secret Service

Sawmill

- Tool to assist an analyst in parsing network text logs
- Processes various text logs generated by a variety of network security devices
- Converts text logs to a cross-linked report that allows analysts to customize the report according to output requirements
- Provides functionality for organizing logs into an easy-to-read report



*U.S. Department of
Homeland Security*

United States
Secret Service

Download Information

- Sawmill can be purchased and downloaded from:
<http://www.sawmill.net>
- Initial download and installation comes with a 30 day, unlimited profile license



*U.S. Department of
Homeland Security*

United States
Secret Service

Procedure: Installing and Configuring Sawmill

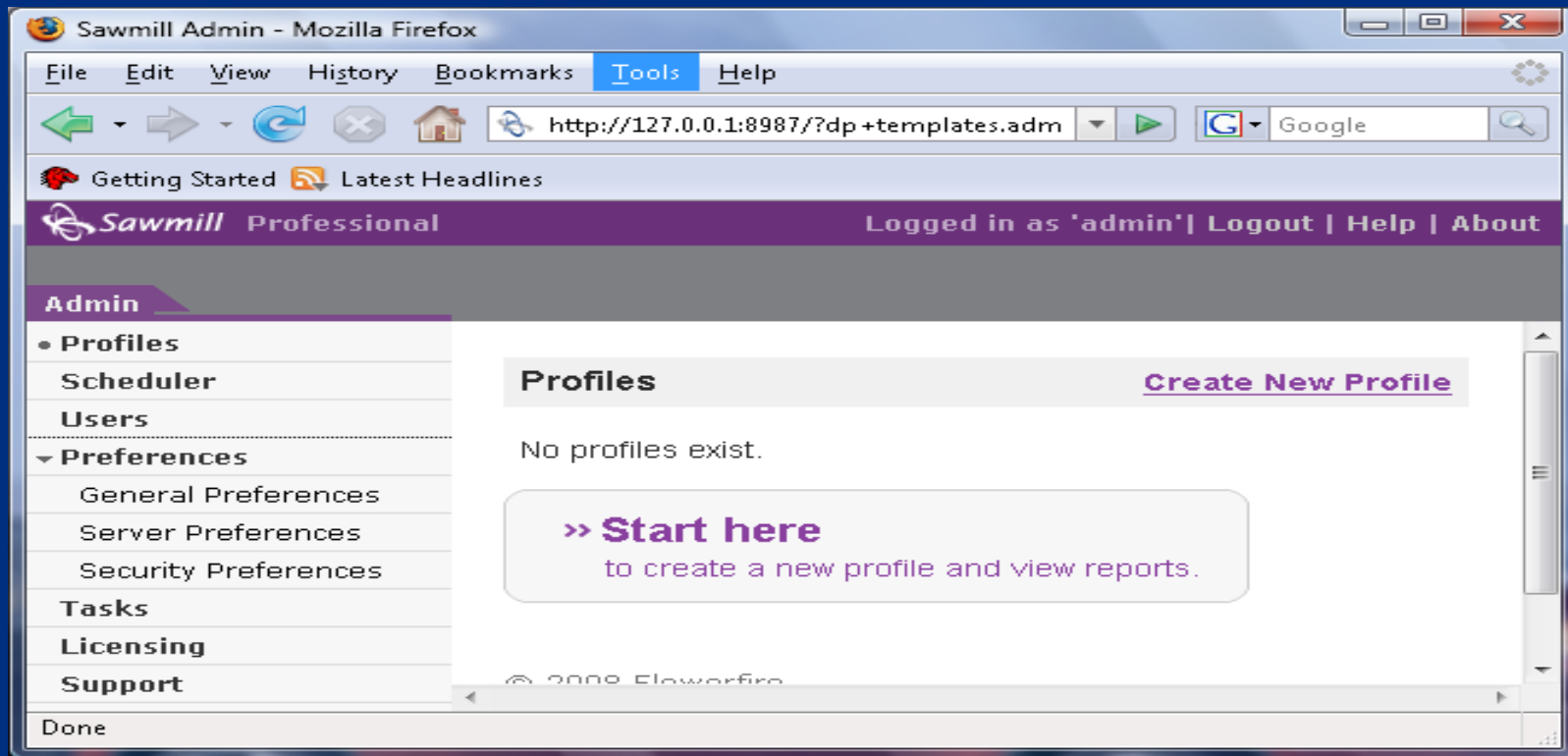
- This is a Step / Action exercise in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

The Administrative Interface



U.S. Department of
Homeland Security

United States
Secret Service

Procedure: Creating a Report Profile

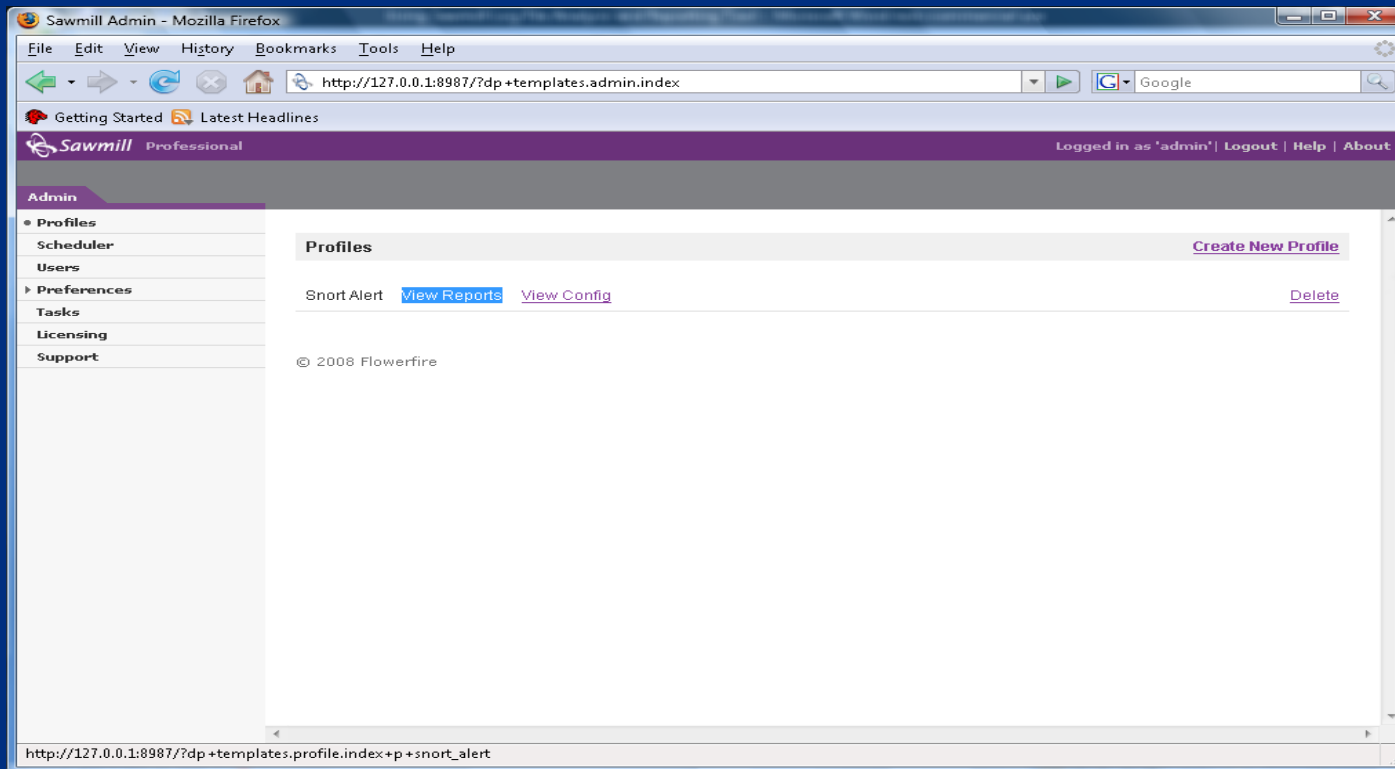
- This is a Step / Action exercise in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

The Report Environment



*U.S. Department of
Homeland Security*

United States
Secret Service

Report Header

- Profile name – Name of active profile which is being displayed
- Admin link – Link to administrative functions, such as profile lists
- Logout – A link to log out of Sawmill
- Help – Help documentation



*U.S. Department of
Homeland Security*

United States
Secret Service

Sawmill's Administrative Interface

The screenshot shows the Sawmill Reports web application running in Mozilla Firefox. The browser's address bar displays the URL: `http://127.0.0.1:8987/?dp+templates.profile.index+p+snort_alert`. The application's header includes the title "Sawmill Reports | Snort Alert - Mozilla Firefox" and a navigation menu with links for "File", "Edit", "View", "History", "Bookmarks", "Tools", and "Help". Below the header, there is a status bar indicating the user is logged in as "admin" with links for "Admin", "Logout", "Help", and "About". The main content area is titled "Overview" and displays statistics for the period "17/Dec/2008 - 20/Dec/2008, 4 days". A table shows the number of events and the average per day. The footer of the application indicates the copyright year 2008 and the name Flowerfire.

Getting Started Latest Headlines

Sawmill Professional Profile: Snort Alert Logged in as 'admin' | Admin | Logout | Help | About

Reports Config

Calendar Date Range Filter Printer Friendly Update Database | Rebuild Database

Overview

Statistics for 17/Dec/2008 - 20/Dec/2008, 4 days ☐ Date Filter ☐ Filter Refresh

	All days	Average per day
Events	370	92.50

© 2008 Flowerfire

Done



U.S. Department of
Homeland Security

United States
Secret Service

Report Toolbar

- Reports - Used to access other loaded reports from current reports view
- Config – Used to change profile options
- Calendar – Date/time filter can be set to view single day, month or year
- Date Range – Range of days can be selected to use as date/time filter
- Filter – Used to configure global filter options for any of report fields, dynamically affect all reports



*U.S. Department of
Homeland Security*

United States
Secret Service

Report Menu

Sawmill Reports | Snort Alert - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://127.0.0.1:8987/?dp+templates.profile.index+p+snort_alert

Getting Started Latest Headlines

Sawmill Professional Profile: Snort Alert Logged in as 'admin' | Admin | Logout | Help | About

Reports Config

Calendar Date Range Filter Printer Friendly Update Database Rebuild Database

Overview

► Date and time

Source hosts

Destination hosts

Source ports

Destination ports

• Events

Protocols

Classifications

Priorities

Types

Codes

Xrefs

TTLs

Type of services

IDs

ACKs

Events

Statistics for 17/Dec/2008 - 20/Dec/2008, 4 days ☐ Date Filter ☐ Filter Refresh

Events Row Numbers Zoom Options Export Table Options

Row 1 - 10 of 14 11-14 > Start row: 1 Number of rows

Event	Events	0 - 100 %
1 [http_inspect] DOUBLE DECODING ATTACK	95 25.7 %	
2 ORIGINAL DATAGRAM DUMP	76 20.5 %	
3 ICMP Destination Unreachable Port Unreachable	51 13.8 %	
4 DNS SPOOF query response with TTL of 1 min. and no authority	37 10.0 %	
5 [http_inspect] OVERSIZE REQUEST-URI DIRECTORY	32 8.6 %	
6 ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	22 5.9 %	

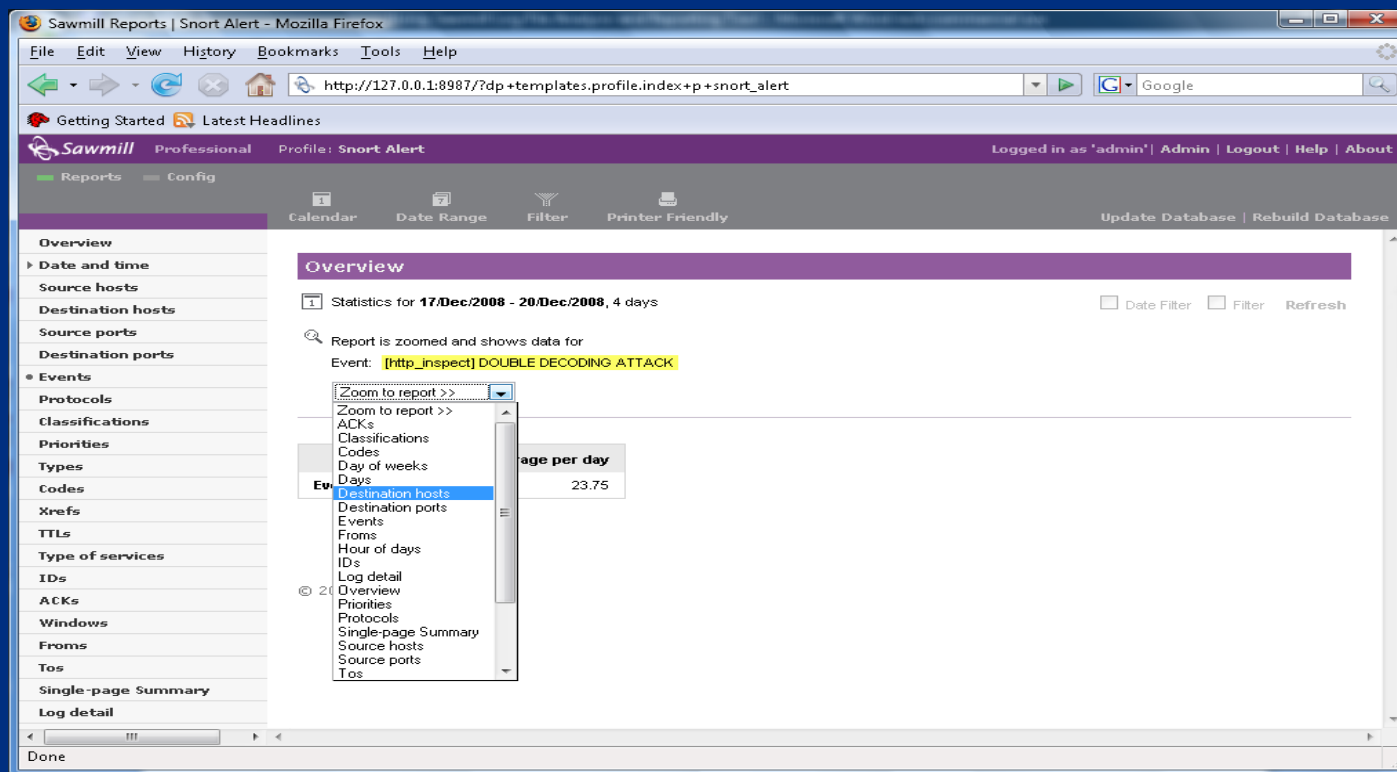
Done



U.S. Department of
Homeland Security

United States
Secret Service

Zoom To Filters



U.S. Department of
Homeland Security

United States
Secret Service

Final Output Report (Log Detail)

Sawmill Reports | Snort Alert - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://127.0.0.1:8987/?dp+templates.profile.index+p+snort_alert

Getting Started Latest Headlines

Sawmill Professional Profile: Snort Alert

Logged in as 'admin' | Admin | Logout | Help | About

Reports Config

Calendar Date Range Filter Printer Friendly

Update Database Rebuild Database

Overview

Statistics for 17/Dec/2008 - 20/Dec/2008, 4 days

Report is zoomed and shows data for

Event: [http_inspect] DOUBLE DECODING ATTACK

Zoom to report >>

Zoom to report >>

ACKs

Classifications

Codes

Day of weeks

Days

Destination hosts

Destination ports

Events

Froms

Hour of days

IDs

Log detail

Overview

Priorities

Protocols

Single-page Summary

Source hosts

Source ports

Tos

Row Numbers

Zoom Options

Export

Table Options

Start row: 1

Number of rows

			Destination host	Source port	Destination port	Event	Protocol	From	To
1			64.156.13.20	1716	80	[http_inspect] DOUBLE DECODING ATTACK	TCP	10.3.20.80:1716	64.156.13.20:80
2			64.236.29.63	1212	80	[http_inspect] DOUBLE DECODING ATTACK	TCP	10.3.20.80:1212	64.236.29.63:80
3	17/Dec/2008 15:07:30	10.3.20.80	64.236.29.63	1521	80	[http_inspect] DOUBLE DECODING ATTACK	TCP	10.3.20.80:1521	64.236.29.63:80
4	17/Dec/2008 16:04:34	10.3.20.80	128.241.21.163	1209	80	[http_inspect] DOUBLE DECODING ATTACK	TCP	10.3.20.80:1209	128.241.21.163:80

Done



U.S. Department of
Homeland Security

United States
Secret Service

Final Output Report, cont'd

Sawmill Reports | Snort Alert - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://127.0.0.1:8987/?dp+templates.profile.index+p+snort_alert

Getting Started Latest Headlines

Sawmill Professional Profile: Snort Alert Logged in as 'admin' | Admin | Logout | Help | About

Reports Config

Calendar Date Range Filter Printer Friendly Update Database Rebuild Database

Overview

Statistics for 17/Dec/2008 - 20/Dec/2008, 4 days

Report is zoomed and shows data for

Event: [http_inspect] DOUBLE DECODING ATTACK

Zoom to report >>

Log detail

Row Numbers Zoom Options Export Table Options

Row 1 - 10 of 95 11-20 > >>> Start row: 1 Number of rows: 10

	Date/time	Source host	Destination host	Source port	Destination port	Event	Protocol	From	To
1	17/Dec/2008 10:53:22	10.3.20.80	64.156.13.20	1716	80	[http_inspect] DOUBLE DECODING ATTACK	TCP	10.3.20.80:1716	64.156.13.20:80
2	17/Dec/2008 13:55:11	10.3.20.80	64.236.29.63	1212	80	[http_inspect] DOUBLE DECODING ATTACK	TCP	10.3.20.80:1212	64.236.29.63:80
3	17/Dec/2008 15:07:30	10.3.20.80	64.236.29.63	1521	80	[http_inspect] DOUBLE DECODING ATTACK	TCP	10.3.20.80:1521	64.236.29.63:80
4	17/Dec/2008 16:04:34	10.3.20.80	128.241.21.163	1209	80	[http_inspect] DOUBLE DECODING ATTACK	TCP	10.3.20.80:1209	128.241.21.163:80

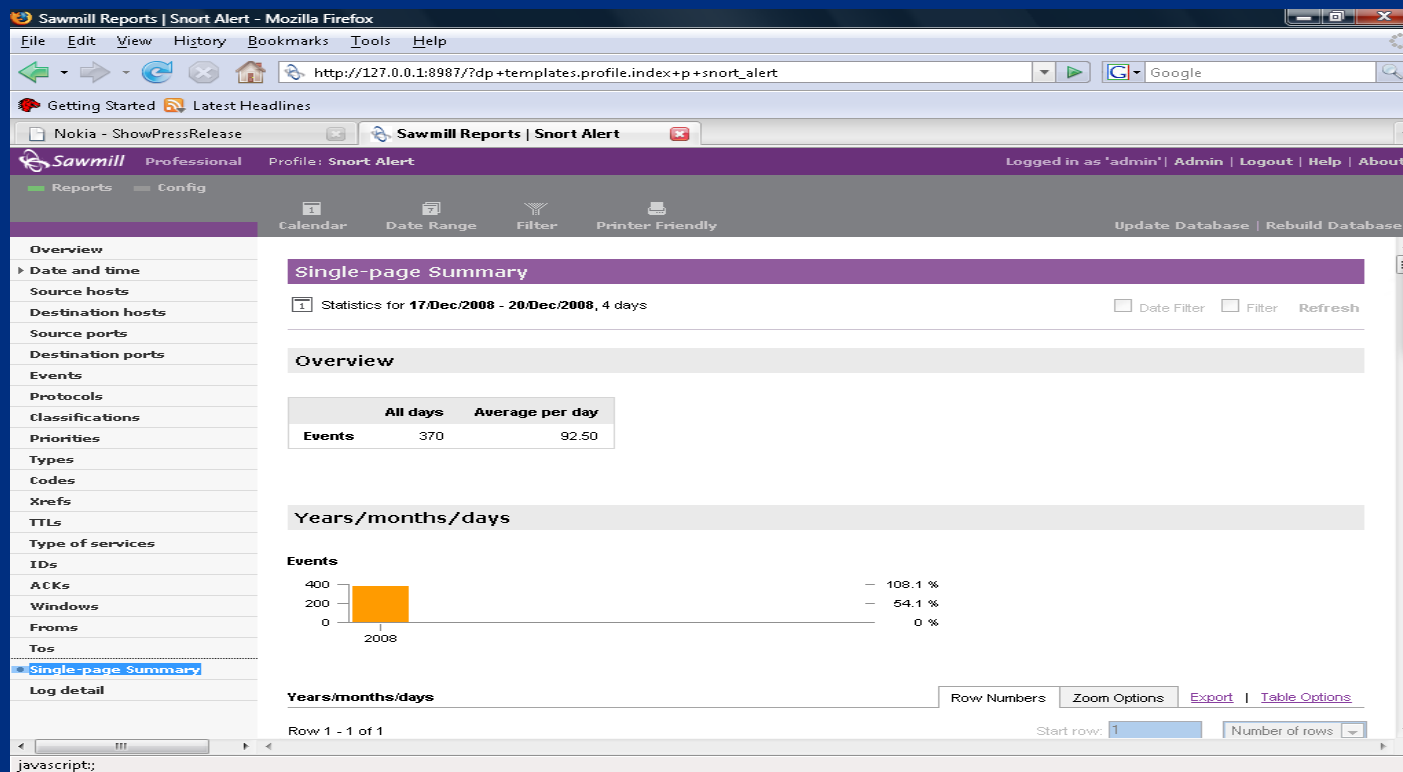
Done



U.S. Department of
Homeland Security

United States
Secret Service

Single Page Summary



U.S. Department of
Homeland Security

United States
Secret Service

Module 15 – Live Data Collection and Analysis



*U.S. Department of
Homeland Security*

United States
Secret Service

You Will Learn . . .

- Data Collection
- Introduction to LiveWire
- LiveDiscover
- LiveWire – Initial inquiry
- LiveWire – Evidence Collection
- LiveWire – Malicious Code Analysis
- Alternate Data Collection Tools



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 1 – Data Collection

- Locating Physical Devices in Server Environment
- Attaching Storage Equipment



*U.S. Department of
Homeland Security*

United States
Secret Service

Network Architecture

- Logical topology map shows how devices connected logically, not necessarily physically
- Network architecture indicates where devices are physically located
- Network devices that provide possible path for incident are considered to be “in-line” to investigation
- Devices that carried traffic relating to incident, may hold crucial information, should be located and analyzed



*U.S. Department of
Homeland Security*

United States
Secret Service

Logical Assessment

- Logical assessment involves obtaining network topologies to get rough estimate of where sensors can be placed for investigation
- Network topology maps may not exist or be severely outdated
- Investigator can update topology through interviews or by performing a physical assessment



*U.S. Department of
Homeland Security*

United States
Secret Service

Physical Assessment

- Includes tracing wire and cable to physical components on network to create a wiring diagram
- Wiring diagram shows physical connections between devices onsite and can help determine accuracy of logical assessment
- Investigator can use several cable testing devices, like a tone generator, to verify cable locations



*U.S. Department of
Homeland Security*

United States
Secret Service

Physical Assessment

- In large network environments, servers and network devices are assigned some form of inventory control, such as bar code or unique name
- May be necessary to search through rows of server racks to locate an identification tag on server of interest



*U.S. Department of
Homeland Security*

United States
Secret Service

Physical Site Examination

- Examine physical site to determine physical data paths and relationship to overall physical environment
- Understanding relationships provides basis for determining what is or is not physically possible on network



*U.S. Department of
Homeland Security*

United States
Secret Service

Physical Site Examination

- Physically locate target host
- Physically locate device to which target host is connected
- Physically locate devices that fall into path of investigation
- Verify network documentation (if available)



*U.S. Department of
Homeland Security*

United States
Secret Service

Verifying Network Configuration

- Investigator needs a starting point to verify network setup and actual location of network devices for an unfamiliar network
- Almost every network has connection to Internet or some external network
- External link typically best starting point to begin tracing wire



*U.S. Department of
Homeland Security*

United States
Secret Service

Verifying Network Configuration

- Tracing wire used to determine how devices are physically connected
- If wire cannot be traced other devices like a network tone generator can be used to determine its termination location
- Use of some devices could require unplugging cable and severing existing connections
- Could alert suspect(s) of ongoing investigation



*U.S. Department of
Homeland Security*

United States
Secret Service

Physically Locating Target Host

- Collect all identifying information regarding device from review of network documentation and interview with system administrator
- Use information and physical assessment of network to locate device



*U.S. Department of
Homeland Security*

United States
Secret Service

Physically Locating Nearest Device

- Use identifying information obtained during review of network documentation
- Record termination location for each network-capable cable connected to machine
- Could be RJ45 or RJ11 socket on nearest wall, hub or switch, or some other device
- If cable terminates at wall socket, record socket's ID number and locate it on patch panel that aggregates cables for that area of facility



*U.S. Department of
Homeland Security*

United States
Secret Service

Data Storage

- Many investigations result in large evidence files that must be collected
- Sufficient data storage to copy and preserve evidence files is imperative
- Retrieved data should always be redirected to forensically clean evidence collection drive
- Never save output of investigation to local system's hard drive, may compromise evidence and could potentially fill computer's disk space



*U.S. Department of
Homeland Security*

United States
Secret Service

Data Storage

- Storage equipment can connect to collection machine by many different connection types
- Common types are: USB, Firewire, and eSATA
- External hard drives with these configurations come in many different capacities
- General rule is to allocate as much disk space as possible for each investigation



*U.S. Department of
Homeland Security*

United States
Secret Service

Wiping and Verification

- Evidence should be stored on a forensically clean drive
- Evidence storage drive must be thoroughly wiped
- Overwriting every bit on drive using known character or set of characters
- Process should be verified to ensure success
- Failure to complete process can result in claims of contaminated evidence, jeopardizing credibility of evidence



*U.S. Department of
Homeland Security*

United States
Secret Service

Wiping Guidelines

- Clearly identify media to be wiped and segregate from other media
- Have only essential media in system during wiping operations
- Ensure correct media selected before executing wipe utility
- Remove wiped media from machine immediately after wiping and store separately
- Annotate in case notes media wiped prior to use
- Label media with software version and command line used



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 2 – Introduction to LiveWire

- Live Digital Investigations
- LiveWire Installation
- LiveDiscover Installation
- Updating LiveWire
- Updating LiveDiscover
- LiveWire Initial Setup



*U.S. Department of
Homeland Security*

United States
Secret Service

Live Digital Investigations

- Traditional computer examinations examine media from a system that has had power removed, or dead-box
- Live Digital Investigations performed on running systems prior to removal of power



*U.S. Department of
Homeland Security*

United States
Secret Service

Why Live?

- Ever increasing use of memory resident programs and utilities revert to obfuscated or encrypted state at power off
- Becoming necessary to seize information from volatile areas BEFORE plug is pulled



*U.S. Department of
Homeland Security*

United States
Secret Service

Reasons for a Live Investigation

- Rapid response requires remote investigation
- Network size limits flexibility
- Encrypted file system requires live capture
- System of interest is mobile
- Commercial system cannot be shutdown



*U.S. Department of
Homeland Security*

United States
Secret Service

How LiveWire Works

- Complex series of scripts, programs and tools
- Uses customized version of Apache web server on investigation system to provide menus, displays and reports in a graphic user interface
- Includes embedded version of Gargoyle malware detection software, also a product of Wetstone
- Requires administrative privileges to access and retrieve data from a target system



*U.S. Department of
Homeland Security*

United States
Secret Service

How LiveWire Works

- Uses a Connect-Act-Disconnect model for communicating with a host on network
- Software logs into target, obtains information and logs out of system



*U.S. Department of
Homeland Security*

United States
Secret Service

Risks

- Use of Livewire can be detected on target
- Could compromise clandestine operation
- User on target system may notice degradation of network performance for short period
- Use may be noticeable as process running in Task Manager of target



*U.S. Department of
Homeland Security*

United States
Secret Service

Minimum Requirements

- Microsoft Windows XP
- 100 Meg Bytes of free disk space
- 128 Meg Bytes RAM
- Pentium 200 Mhz
- Network Interface Card
- CD ROM Drive for Installation
- VGA Resolution Monitor
- Mouse



*U.S. Department of
Homeland Security*

United States
Secret Service

Procedure: LiveWire Installation

- This is a Step / Action in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

Procedure: Installation of LiveDiscover

- This is a Step / Action in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

Procedure: Updating LiveWire

- This is a Step / Action in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

Procedure: Updating LiveDiscover

- This is a Step / Action in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

LiveWire Initial Setup

- Setup Administrator account
- Create an Investigator account



*U.S. Department of
Homeland Security*

United States
Secret Service

Procedure: LiveWire Setup

- This is a Step / Action in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 3 – LiveDiscover

- LiveDiscover Network Scanning



*U.S. Department of
Homeland Security*

United States
Secret Service

LiveDiscover

- Used to rapidly identify and assess resources on network
- Information gathered used to enable LiveWire tools to perform live analysis of machine across a network
- Can quickly scan single target or whole range of IP addresses
- Performs in-depth scan to include report of vulnerabilities of systems
- Each scan stored and saved in its own database



*U.S. Department of
Homeland Security*

United States
Secret Service

LiveDiscover Interface

- Provides tabbed interface for navigation
- Primary tabs displayed horizontally across top of page
- Each page displays information or options pertaining to specific details or configurations



*U.S. Department of
Homeland Security*

United States
Secret Service

Interface Tabs

- Discovery Tab - input for addresses to be scanned, up to four different network ranges can be scanned at same time
- Network Tab - tree structure created showing different devices discovered for subnet as well as detailed information gathered about devices
- Responses Tab - displays discovered data grouped together, selecting any options displays all items found matching criteria



*U.S. Department of
Homeland Security*

United States
Secret Service

Interface Tabs

- Reports Tab - facilitates generation of many different report display formats, reports can contain text as well as colored graphs
- Script Tab - accesses different pre-built discovery scripts stored in database, customized scripts can be added
- Settings Tab - contains configurations used during live discovery process
- Utilities Tab - options for scripts and results from other scans to be imported into the current database



*U.S. Department of
Homeland Security*

United States
Secret Service

Performing a LiveDiscovery Network Scan

- This is a Step / Action in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 4 -Volatile Data Analysis

- LiveWire Initial Inquiry
- System State
- Current User Activity
- Active Network State



*U.S. Department of
Homeland Security*

United States
Secret Service

Initial Inquiry

- First part of process when performing investigation or analysis of system using LiveWire
- Will retrieve available information from remote computer at time of scan
- Has potential to degrade performance on target system
- Could alert user of activity on his or her system
- Advanced user may be able to determine analysis taking place



*U.S. Department of
Homeland Security*

United States
Secret Service

Performing LiveWire Initial Inquiry

- This is a Step / Action in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

LiveWire – Display Acquired System State Summary

- This is a Step / Action in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

LiveWire – Acquire Physical RAM and Registry

- This is a Step / Action in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

LiveWire – Current User Activity

- This is a Step / Action in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

Display Captured Network Details

- This is a Step / Action in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 5 – Evidence Collection

- File System Status
- Physical vs. Logical
- Collection and Preservation
- Hashing



*U.S. Department of
Homeland Security*

United States
Secret Service

Procedure: Capture Disk Information

- This is a Step / Action in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

Body File Acquisition

- This is a Step / Action in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

Physical vs. Logical Image

- Physical image is a bit-for-bit duplicate of a media storage device
- A logical image only contains data from the active file system of a storage device
- From forensics standpoint, physical image preferable to logical image because it may contain more evidence



*U.S. Department of
Homeland Security*

United States
Secret Service

Physical Images

- Contain information from entire physical device or designated portion of it
- Are not file system-specific
- Capture all sectors within a designated area of a device, both in the system and data areas (including all files, unallocated space, swap space, etc.)
- Are typically placed in an Image file (a logical file that contains the bit-for-bit copy)



*U.S. Department of
Homeland Security*

United States
Secret Service

Physical Imaging

- EnCase
- dcfldd
- Enables recovery for analysis of deleted data or information that resided in slack space on original drive
- Slack space can contain information from whatever previously occupied the space



*U.S. Department of
Homeland Security*

United States
Secret Service

Logical Images

- Only contain information from active file system
- Contain only enough information to reproduce logical volumes or parts of them
- Are file system-specific
- Allow registry and other system files to be backed up, but only if specifically requested



*U.S. Department of
Homeland Security*

United States
Secret Service

Logical Images

- Do not capture slack space, free space, or partition information
- Do not capture files that are open at time of imaging
- Do not capture any files that you do not have access to read
- Do not capture temporary files, such as pagefile.sys, win386.swp, etc.



*U.S. Department of
Homeland Security*

United States
Secret Service

Logical Imaging

- Microsoft's Windows Backup
- Creates image files of an entire active file system
- Logical image only contains active files
- Not possible to recover and analyze any deleted files or slack space



*U.S. Department of
Homeland Security*

United States
Secret Service

On-site Imaging Guidelines

- May face considerable time and material constraints
- May have to perform actions in strange environment with unknown equipment
- Challenges to accomplishing even simple actions, such as finding appropriate settings in BIOS or gaining access to inside of machine
- Preparation helps mitigate problems
- Deviation from general procedures for any reason should be documented



*U.S. Department of
Homeland Security*

United States
Secret Service

Physical Disk Imaging

- This is a Step / Action in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

Collecting Files

- This is a Step / Action in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

LiveWire Hashing

- LiveWire uses MD5 for hashing
- MD5 (Message Digest 5) creates a 128-bit message digest that is “unique” to message
- MD5 is currently accepted standard for verification by majority of computer forensic community



*U.S. Department of
Homeland Security*

United States
Secret Service

Hashes Defined

- Hash (or message digest) is a numerical value generated by applying a mathematical algorithm against a data set
- Hashing algorithms take variable length input and output a “unique” fixed-length result
- Nearly impossible to find two different data sets that naturally have same hash values
- Hash value analogous to fingerprint of file
- File hash value can be used to identify file no matter where found



*U.S. Department of
Homeland Security*

United States
Secret Service

Hashes Defined

- If file's data does not change in any way, same algorithm can be applied infinite number of times, resulting alphanumeric values will never change
- If hash value does change, it can be assumed file has been modified
- Comparing hash values is excellent way to check integrity of files
- Hashing algorithms are “one-way” can be created from file or device data, but cannot recreate data from hash



*U.S. Department of
Homeland Security*

United States
Secret Service

Generating Hashes for the Inquiry

- This is a Step / Action in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 6 - Malicious Code Analysis

- Malicious Program Search



*U.S. Department of
Homeland Security*

United States
Secret Service

Types of Malicious Programs

- Many different types of malicious programs and categories
- Many programs may not show that machine was compromised but could hint about interests or intentions of user
- Types of programs on machine could identify personality of user, could indicate expertise and guide investigator's search
- For instance, if encryption program such as TrueCrypt found, should raise concern that encrypted volumes may be present and may be hiding critical evidence



*U.S. Department of
Homeland Security*

United States
Secret Service

Malicious Code Scans

- LiveWire has ability to search many different categories of malicious code
- LiveWire scans compare hash signatures of files on system against the National Software Reference Library (NSRL) database
- The NSRL is a free database released by National Institute of Standards and Technology (NIST)



*U.S. Department of
Homeland Security*

United States
Secret Service

Common Malicious Code Categories

- Anti Forensics
- Encryption
- Key Loggers
- P2P Tools



*U.S. Department of
Homeland Security*

United States
Secret Service

Common Malicious Code Categories

- Password crackers
- Rootkits
- Steganography
- Wireless



*U.S. Department of
Homeland Security*

United States
Secret Service

Malicious Program Search

- This is a Step / Action in student book.



*U.S. Department of
Homeland Security*

United States
Secret Service

Lesson 7 – Alternate Data Collection Tools

- Windows Forensic Toolkit
- Helix



*U.S. Department of
Homeland Security*

United States
Secret Service

Sysinternals - PsTools

- Utilities developed by Mark Russinovich
- Collection of tools capable of performing many different analysis functions on local or remote systems
- Latest version of collection can be downloaded from Microsoft.com



*U.S. Department of
Homeland Security*

United States
Secret Service

psinfo.exe

- Retrieves system information on target system
- Uptime
- Kernel version
- Product type
- Service pack
- Kernel build number



*U.S. Department of
Homeland Security*

United States
Secret Service

psinfo.exe

- Registered organization
- Register owner
- Install date
- IE version
- System root



*U.S. Department of
Homeland Security*

United States
Secret Service

psinfo.exe

- Processors
- Processor speed
- Processor type
- Physical memory
- Video driver



*U.S. Department of
Homeland Security*

United States
Secret Service

pslist.exe

- Lists processes currently running on remote system



*U.S. Department of
Homeland Security*

United States
Secret Service

psloggedon.exe

- Displays list of currently logged on users on remote system for both local and remote users



*U.S. Department of
Homeland Security*

United States
Secret Service

psexec.exe

- Advanced utility used to execute commands on remote system
- Ability to copy a program from local system to remote target and execute program interactively



*U.S. Department of
Homeland Security*

United States
Secret Service

psfile.exe

- Used to view files that are opened remotely on target system



*U.S. Department of
Homeland Security*

United States
Secret Service

psgetsid.exe

- Retrieves SID of target system



*U.S. Department of
Homeland Security*

United States
Secret Service

psloglist.exe

- Retrieves logs from target system
- By default psloglist.exe will show contents of System event log
- Application, security, or other log can be retrieved if specified



*U.S. Department of
Homeland Security*

United States
Secret Service

psservice.exe

- Retrieves list of running services on target system



*U.S. Department of
Homeland Security*

United States
Secret Service

Helix Live CD

- Specially customized distribution of Knoppix created and maintained by e-fense, Inc.
- Geared toward forensics and incident response
- Created to be used as internal tool for incident response and forensics to create forensically sound images
- Released to public November 2003
- Two different operating modes, Windows and Linux



*U.S. Department of
Homeland Security*

United States
Secret Service

Helix Windows Mode

- Created with Windows executables and contains many tools for incident response on Windows machines
- Runs standard windows applications to gather information from a “Live” running system
- Useful where systems cannot be shut down or where potential evidence would be destroyed by taking system offline
- Helix will make changes to system, exact use should be documented



*U.S. Department of
Homeland Security*

United States
Secret Service

Helix Windows Mode

- To use, place CD in target system
- Click Accept on initial warning screen as displayed on the following slide



*U.S. Department of
Homeland Security*

United States
Secret Service

Helix Windows Mode



U.S. Department of
Homeland Security

United States
Secret Service

Helix Windows Mode

- After accepting Warning, the screen on the following slide will be displayed
- Icons on left side of window can be selected for use of associated functions
- The toolbar also contains options that will provide access to data collection functions
- Use Quick Launch and Win Audit option on toolbar to acquire information on Windows system quickly and easily



*U.S. Department of
Homeland Security*

United States
Secret Service

Helix Windows Mode



*U.S. Department of
Homeland Security*

United States
Secret Service

Helix Windows Mode

- Another feature of windows mode is ability to acquire images of live system
- Can be done using Live Acquisition feature of CD
- Image physical memory, physical drive, or logical partitions
- Save images to attached device, network share or to evidence capture machine using NetCat



*U.S. Department of
Homeland Security*

United States
Secret Service

Helix Windows Mode



U.S. Department of
Homeland Security

United States
Secret Service

Helix Windows Mode

- FTK Imager also available on CD to create forensic images, can save in different formats such as raw dd and E01 (encase) images
- Located on menu bar under Quick launch > FTK Imager
- FTK Imager allows for imaging physical and logical drives



*U.S. Department of
Homeland Security*

United States
Secret Service

Helix Windows Mode

Tools Available in Windows Mode		
Command Shell	FTK Imager	Sys Info Viewer
Drive Manager	Win Audit	Zero View
Per-Search	WFT	NetCat
VNC Server	PuttySSH	File Recovery
Rootkit Revealer	Screen Capture	Password Viewers



*U.S. Department of
Homeland Security*

United States
Secret Service

Helix - Linux Live CD Mode

- Linux mode of Helix is pure Live CD that allows for “dead box” forensics
- Allows user to investigate computer system without forensically changing any data on drive
- Many tasks can be carried out with Helix, such as forensically duplicating disks and analyzing the forensic disk images
- To start Helix in Linux mode system will need to be booted to the bootable Helix CD
- BIOS on motherboard must be configured properly



*U.S. Department of
Homeland Security*

United States
Secret Service

Linux Disk Mounting and Imaging

- When Helix is booted into Linux mode, it automatically mounts storage devices in read only mode
- Will also mount devices with noatime option, prevents change to access times of files stored on disk
- Helix mounts drives read-only by default, but can be forced to mount devices read-write by typing:

```
mount -rw <device> <mount point>
```



*U.S. Department of
Homeland Security*

United States
Secret Service

Linux Disk Mounting and Imaging

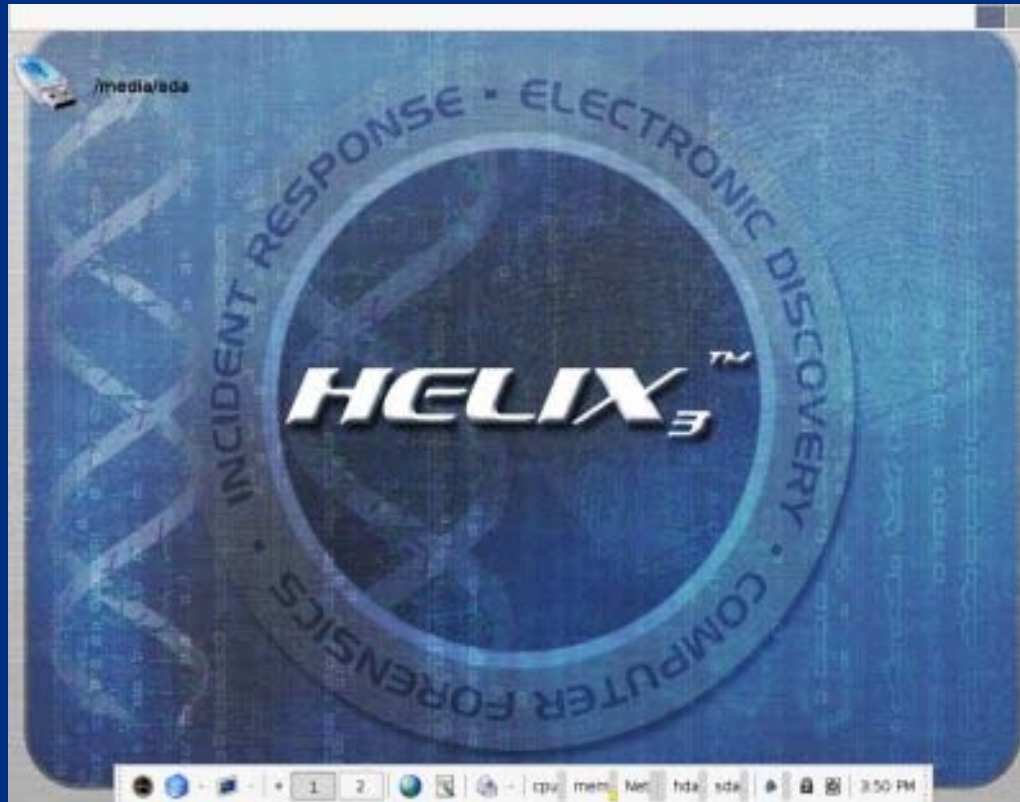
- Once Helix fully booted, screen will appear similar to image on next slide
- Will show a list of all storage media mounted on left side of screen
- Task bar located at bottom of screen
- “Start” menu is icon of Helix CD cover



*U.S. Department of
Homeland Security*

United States
Secret Service

Helix Default Screen



*U.S. Department of
Homeland Security*

United States
Secret Service

Linux Disk Mounting and Imaging

- Several GUI utilities included on disk for creating forensically sound images such as Adepto, Air, and Linen



*U.S. Department of
Homeland Security*

United States
Secret Service

Linux Live CD Forensic Tools

- Helix provides tools for investigating collected disk images
- Autopsy, shown on next slide, is popular Linux tool for viewing and searching images
- Autopsy is GUI interface to suite of command line forensic tools named The Sleuth Kit



*U.S. Department of
Homeland Security*

United States
Secret Service

Autopsy Default Screen



*U.S. Department of
Homeland Security*

United States
Secret Service

Linux Live CD Forensic Tools

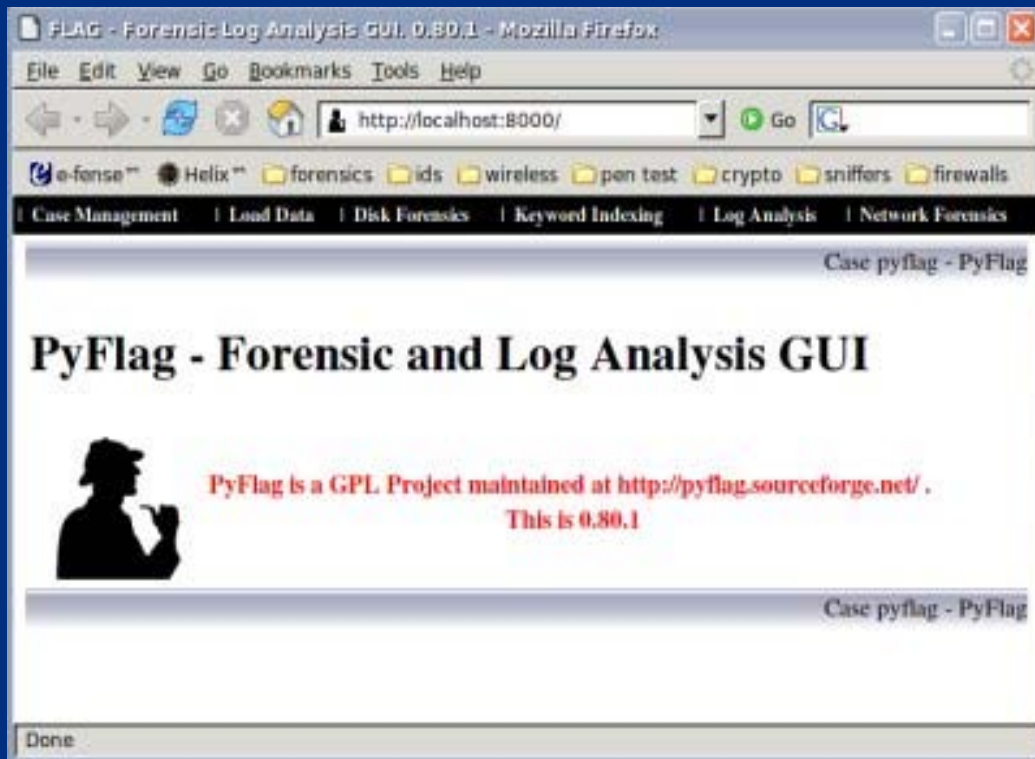
- Another option available is PyFlag
- Fforensic and log analysis application created by Australian Department of Defense
- PyFlag uses backend database to assist managing large amounts of data, web driven, can be deployed on central server and used by several users at same time
- PyFlag able to examine forensic evidence from disk images, logs, and network captures



*U.S. Department of
Homeland Security*

United States
Secret Service

PyFlag Default Screen



*U.S. Department of
Homeland Security*

United States
Secret Service

Live CD Benefits

- Useful for testing, evaluating, or learning without need of dedicated hardware
- Many Linux distributions available as Live CDs, freely downloaded from Internet, each designed for specific task
- Helix just one example of feature rich Live CD created for a certain purpose, forensics and incident response
- Helix provides multiple options for investigations whether suspect machine turned off or up and running



*U.S. Department of
Homeland Security*

United States
Secret Service



*U.S. Department of
Homeland Security*

United States
Secret Service